MANAGING CYBER OPERATOR TRAINING CIRRICULUM

GRADUATE RESEARCH PROJECT

Matthew G. Beach, Major, USAF

AFIT/ICW/ENG/10-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

Report Documentation Page

Form Approved
OMB No. 0704-0188

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

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Managing Cyber Operator Training Curriculum	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) **Air Force Institute of Technology,2950 Hobson Way,WPAFB,OH,45433-7765**	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

The purpose of this research was to examine the state of various training programs existing for communications officers, and new training being developed for the new 17D cyber operator career field. The methodology for this project consisted of a review of existing training plans for communications officers, a review of course design documentation for new course development efforts, a review of the new career training plan, and a review of the content of the 33S to 17D transition course (X-Course). These materials were reviewed and potential problem areas were identified.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**56**	

The views expressed in this report are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government

AFIT/ICW/ENG/10-01

MANAGING CYBER OPERATOR TRAINING CIRRICULUM

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Systems and Engineering and Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Masters of Cyber Warfare

Matthew G. Beach, BS

Major, USAF

June 2010

AFIT/ICW/ENG/10-01

MANAGING CYBER OPERATOR TRAINING CIRRICULUM

Matthew G. Beach, BS
Major, USAF

Approved:

_____/signed_____ _____
Robert F. Mills, PhD (Chairman) Date

_____/signed_____ _____
Harold J. Arata, Col, USAF, PhD (Member) Date

Abstract

The purpose of this research was to examine the state of various training programs existing for communications officers, and new training being developed for the new 17D cyber operator career field. The methodology for this project consisted of a review of existing training plans for communications officers, a review of course design documentation for new course development efforts, a review of the new career training plan, and a review of the content of the 33S to 17D transition course (X-Course). These materials were reviewed and potential problem areas were identified.

Recommendations resulting from this research project include careful monitoring and comparing of student skill sets coming from the new Undergraduate Computer Training course to ensure new cyber operators are receiving a solid base line of knowledge in their career force accession training. Best practices for the use of Advanced Distributed Learning are presented so they can be incorporated into the training plan. Finally new skill descriptors are recommended for use by the various school houses for their use in developing curriculum that successfully builds on itself as students progress through the courses.

Table of Contents

List of Figures

List of Tables

MANAGING CYBER OPERATOR TRAINING CURRICULUM

I: Overview

Background

The purpose of this Graduate Research Project is to examine training efforts during the transition of Communications Officers to Cyber Operators. Many challenges exist to steer us through this period of changes. The Air Force must be aware of the decisions and choices which have led to this critical moment in the history of the career field. The scope of involvement in the evolution of the cyberspace environment must be determined, skills which support that involvement must be defined, and an effective training model around these skills must be structured.

The Air Force has already begun this process. Indeed training programs have always existed as the career force has changed names and missions. The Air Force is in the midst of another shift in how it organizes, trains and equips its cyber operations force. The shift has gone from a force with diverse responsibilities such as software analysts, mobile communications, executive officers and network specialists.

The Air Force has been constantly developing and refining its training and education program in an attempt to keep up with rapid changes in technology, and now the challenge of shifting a support career field to an operational career field presents an opportunity to also restructure its training program to build a flexible, modular and expandable curriculum to serve the cyber operator career field well into the future.

Problem

The overarching problem explored in this paper is what is the best way to manage training during the transition from 33S to 17D? There are other questions that follow this one. What factors led to the current state of affairs? What is being done now? What skills and training are needed? What are potential problem areas, and how can they be avoided? This paper will follow those questions to explore the current state of Air Force Training and provide suggestions on how to manage it through the transition phase.

Scope

The scope of this research project is focused on officer training through accession and through intermediate and senior officer training for the cyber career field. It will focus on those who have begun the 33S training program who are transitioning to the new 17D career field, and those entering as brand new 17Ds. It will focus on existing courseware, and new courseware slated to be released in the coming year. It will cover use of Advanced Distributed Learning (ADL) as prerequisites to these courses and as a tool for transition training.

Outline

This paper will follow the questions outlined in the above problem statement. It asks the main question: How can the Air Force best manage its transition training for 17Ds? The question how we got here will be examined. A look at the necessary skills

will follow. A section on the state of Air Force training efforts will follow. The last two chapters explore potential problem areas and suggested methods to mitigate these pitfalls.

II: History

This chapter contains an overview of how the Air Force migrated from a support mindset to an operational focus with regard to cyber operations. During this evolution, many intermediate changes were made to the career field creating an environment where many communications officers have vastly different skill sets. During this time there have been discussions about outsourcing the career field and reducing the number of communications officers; but at the same time we have been working hard to operationalize and professionalize the network and create a new career field. This brings us to where we are now, standing up a new organization for conducting cyber operations, transitioning communications officers to a new career field, and beginning to conduct training for this new career force.

The Communications Career Field in the 90s

In the early 1990s the communications career field looked very different then it does now. The career force has changed as the Air Force's knowledge and attitude towards information technology has evolved. The 90's saw a migration from custom military designed and developed solutions for software and hardware shift toward Commercial Off The Shelf (COTS) products. This attitude carried over to the way the career field was managed and structured as well, culminating with the idea of outsourcing communications functions in the Air Force.

The move to COTS products and services was an overall good idea from an acquisition, operations, and maintenance standpoint. It freed the military from long, costly acquisition cycles and the need to maintain an in-house force of software maintainers. Eventually this decision led to a draw down in the size of the communication career field along with a redistribution of duties.

All the different designators (engineer, plans, maintenance, developer analyst, etc.) were dropped for the communications career field, and every officer was labeled a generic communication officer. This did away with the specialized education requirements needed to obtain these designators. A generic communications officer could expect to do a wide range of duties, to include executive officer and visual information manager.

As these changes were occurring a new development was taking place: the emergence of small networks in the workplace. Desktop personal computers (PCs) became ubiquitous in the new environment. The Air Force embraced this trend, with individual offices developing networks for their own purpose, often unconnected to the other offices in the same building. These networks were set up by local experts and when they changed duty stations or separated these networks could fall into disarray. One thing was evident, once people got used to operating on them, they did not want to go back to the old way of business.

As the number of these network grew and their importance became evident the Air Force recognized the need to standardize the equipment across the enterprise so that skills could be taught to network maintainers who could service the networks whenever they changed duty stations. This led to the creation of the Combat Information Transport

System (CITS), a standardized suite of equipment authorized for use in constructing Air Force networks.

CITS equipment was installed around the Air Force, and a hierarchy of control centers was created. At the base level the, Network Control Center (NCC) housed services for the local base population, including domain control, e-mail, web services and anti-virus systems. The individual bases were accounted for through a system of Network Operations Security Centers located at each MAJCOM. This consolidation was an important step forward for Air Force network operations.

The Drive to Air Force Cyber Command

The field known as Information Warfare has been evolving and maturing since the 1990, and is now defined by three areas, Influence Operations, Electronic Warfare and Network Warfare. The subset of skills compromising Network Warfare includes Network Attack (NetA), Network Defense (NetD) and Network warfare Support (NS). Many of the skills and disciplines used in the Air Force network operations centers overlapped these areas. To differentiate these skills the term NetOps was introduced to include the more management orientated skills such as NetD (the passive element of network defense) and Information Assurance.

At this time Air Combat Command assumed control of Air Force Network Operations and all Network Operations Security Centers (NOSCs) reported to a central Air Force Network Operations Security Center at Barksdale AFB. This consolidation continued as leadership decided to pull functionality from the individual base Network

Control Centers up to the MAJCOM NOSCs. This didn't stop there as the MAJCOM NOSCs were consolidated into Integrated-NOSCs (I-NOSCs), of which there are two: I-NOSC East at Langley AFB and I-NOSC West at Peterson AFB.

In September 2006 the Air Force called for options to stand up and new MAJCOM to be designated Air Force Cyber Command. It was determined that the 8th Air Force would become this command and efforts were begun to develop career paths to support this new MAJCOM. (Franz, 2007)

During this time there were many different opinions on what components would be pulled from Information Operations (IO) to be included in the creation of the new cyber career field. It was clear that Network Operations would be included, but what about Electronic Warfare (EW)? Under the definition of cyber from the National Military Strategy for Cyberspace Operations the cyber domain was "characterized by the use of electronics and the electromagnetic spectrum" (NMS-CO, 2006). The move was underway to pull in the Network Warfare and EW components from IO to the new AFCYBER.

In 2008, leadership changes and new priorities brought the implementation of AFCYBER to a standstill. Cyberspace was still viewed as a high priority, but new leadership believed a new MAJCOM was not necessary. (Shachtman, 2008)

The 24th Air Force

This change in plans resulted not in a new Major Command, but a new numbered Air Force, the 24th Air Force, to be created under Air Force Space Command. The

structure remained similar to what was created for the provisional Air Force Cyber Command. One major change was that EW was no longer considered to be part of cyberspace operations and EW personnel would not be part of the cyber force. IO however went under the new command as the 688 Information Operations Wing (IOW).

The 24th Air Force is composed of three wings. The 688th IOW is responsible for IO and network engineering. The 67th Network Warfare Wing (NWW) is responsible for NetOps and monitoring and Computer Network Defense and Attack. The 689th Combat Communications (CCW) Wing is responsible for providing deployable communications equipment and manpower. (Pampe, 2009)

This describes where the Air Force stands right now. The career field is taking off in a bold new direction. Along with the change in organization there is a new force structure. Communication officers are no longer support personnel, but are now defined as operators. The next chapter discusses the required skills for these organizations.

III: Defining Cyberspace and Determining Skill Requirements for the Cyber Force

The subject of this chapter is defining cyberspace and determining what skills are required for the cyber career force. The Air Force has already collected many desirable skills documents, course training standards and other documentation which define and categorizes skills, but there are overlaps and grey areas which lead to duplication and repetition in some areas of training. There are also gaps that will need to be addressed.

Many factors impact this state of affairs. A clear understanding of cyberspace is still evolving. Only a few years ago each service used its own definition of the environment or domain. The Department of Defense defines cyberspace as "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." (NMS-CO, 2006) Cyberspace operations are defined as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." (AFDD 3-12, 2010) This definition serves as a good common definition of cyberspace and cyber operations, but our understanding of the domain is very immature.

This chapter will outline the broad skills that the Air Force thinks is important for cyberspace. There will be a brief overview of the cyber environment and domain as it is understood today followed by an overview of skills necessary to operate in this domain.

Environments and Domains

Before an entity becomes a war-fighting domain it exists as an environment. "The United States increasingly stresses the concept of cyberspace as an operating environment. The Nation's leaders have begun to recognize the significance of this environment for U.S. security." (Rattray, 2009) Each environment has several properties which define it and describe it. The land domain is characterized by properties that people live on it, people grow their food on it, and people build their communities on it. Its terrain is defined by elevation, features such as forests and desserts. It is also subject to a variety of weather conditions. At some point in the past boundaries of different cultures came into contact, and territories became contested, at which point people tried to take resources from their neighbors. This signified the beginning of armed conflict in the land domain.

When an environment becomes a war-fighting domain it is characterized by the environmental features that affect armed conflict within the domain. Over time, we have developed doctrine and principles on how to best fight in the domain. For example, it is best to hold the high ground, or when faced with a superior force choose terrain that limits the frontage the enemy is able to bring into contact. Thinking of an environment as a domain helps define how best to fight in, win, and achieve superiority of that domain.

Cyber Domain

The cyber environment must be understood before we can adequately describe the cyber domain. The cyberspace environment has both physical and non-physical

components. However, even the physical component can be hard to understand as some of the components cannot be seen or touched, either because it is too small or it exits as waveforms that reside outside the boundaries of human perception. It is an environment that humans control for their purposes and are responsible for establishing it, maintaining it and ultimately destroying it as necessary. The "'geography' of cyberspace is much more mutable than other environments...portions of cyberspace can be turned on and off with the flick of a switch." (Rattray, 2009)

The cyberspace environment exists in the physical world as transmission of electrical signals through a medium. These signals can travel through cables capable of propagating a signal such as fiber-optics or copper wire or they may travel through the air as electromagnetic waves. Examples of these signals through history have been telegraph messages traveling over cooper wire, radio waves propagating through the atmosphere, and telephone signals traveling as electrical waves along copper cable. Electrical charges are passed within the electronic devices that that make up the ever growing number of personal computing devices. All these signals represent control information or data. It is the transmission medium and the information contained in the signals that form the cyber environment.

When the transition from environment to domain is made we have to define what is ours, and what we are trying to do. In the case of the cyber environment we own the information we are sending through cyberspace. We want to maintain the integrity of the information and data so we may use it for our own ends. A state of conflict may exist in which one group may attempt to limit another group's access to their own information, or defend their own information from an adversary.

There are many ways to look at what can be achieved as military goals in cyberspace. We can attack the medium for transmission of the information (e.g., we can cut the wire). We can attack the information itself hoping to corrupt it, either to confuse the purpose or damage it outright. We can seek to achieve effects on the target audience of the information, changing information to hamper their use of the domain by confusing or deceiving them. When describing effects in cyberspace it is clearer to think of it as existing across three separate layers or dimensions. Martin Libicki has labeled these the physical layer, the syntactic layer, and the semantic layer. (Libicki, 2007)

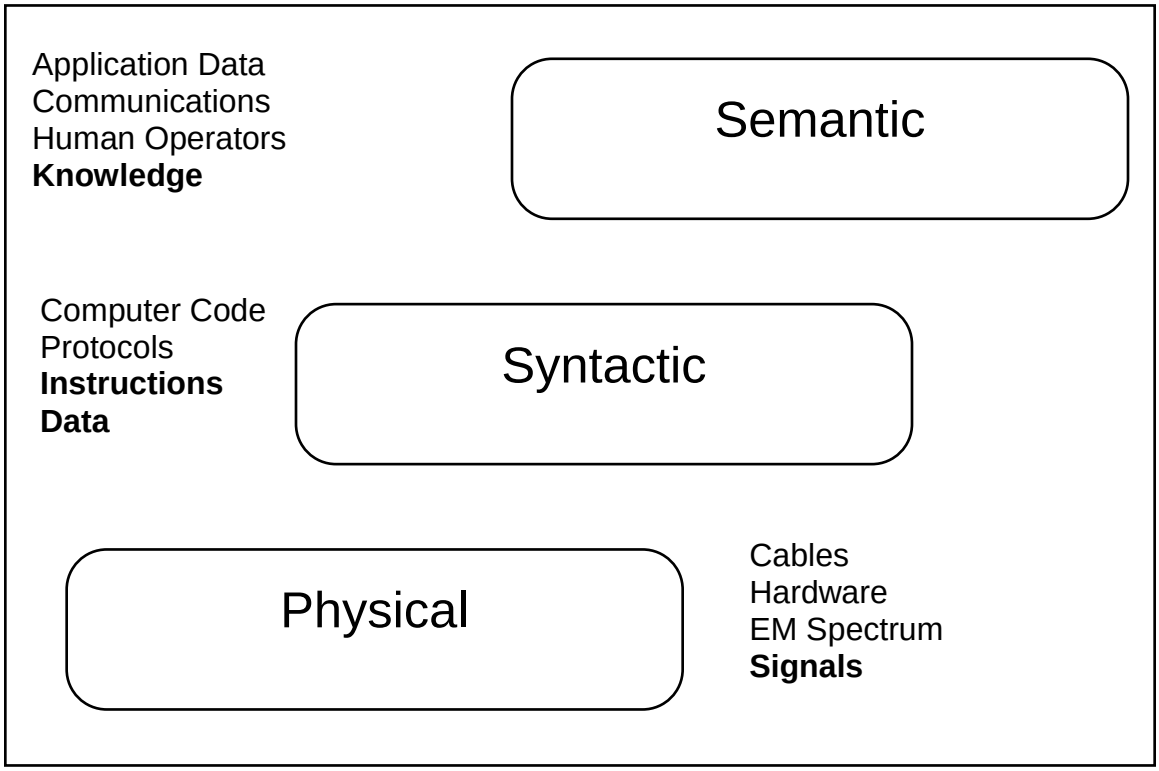

Figure 1. Layers of Cyberspace (Libicki, 2007)

Physical Layer

The physical layer of cyberspace "consists of the various means that permit the circulation of bits...Here one sees wires, routers, computer hardware, ground terminals, antennae, satellites--the works." (Libicki, 2007) This layer compromises the broadcasts into and through the electromagnetic spectrum, and the cable infrastructure for information to flow in our interconnected society.

At this layer people make use of naturally occurring materials and scientific principles to transmit information. Physical devices that can be seen and touched exist in the physical layer. Even though people cannot see radio waves they can see transmission towers, and antennae. The resulting audio messages can be heard coming out of speakers, and images can be displayed on a television screen.

The effects that can be achieved in the physical layer revolve around removing and establishing the capability to transmit our messages. Organizations seek to establish a network over which they can securely and reliably transmit information to achieve an advantage in the decision making process. This is the layer of engineers, communications officers, electronic warfare operators and even pilots dropping bombs to destroy critical nodes of an adversary's networks.

Syntactic Layer

"The syntactic layer of consists of the various instructions and services that tell information systems what to do with information." (Libicki, 2007) This layer consists of all the bits flowing through the transmission mediums and devices of the physical layer.

This information is the heart of cyberspace. This is where man has encoded bits to achieve purpose. These bits are part of control instructions which tell something how to act, or they are data meant to be stored and or displayed for eventual human use; either by human decision makers or other automated information systems.

In this layer voice messages are encoded into logical structures and computer code, taking on many several possible uses according to pre-agreed upon protocols that define their purpose. The machines that act on this information must implicitly trust it as valid control information or sensible data. Humans can craft the information and encode it, but only machines can properly process it at the speed required of today's information systems.

It is this reason that makes the syntactic layer vulnerable. Knowing that the machines must blindly trust the information transiting these networks, humans can take advantage of the rules for their own ends. Skills in programming, engineering, and analysis of traffic and protocols rule this layer of cyberspace.

Semantic Layer

"The semantic layer contains a system's information content." (Libicki, 2007) What is important about this layer is it is where information is acted on by human beings. At the semantic layer the machines blindly pass on their information or follow their instructions like the cold automatons they are. At this level we must introduce a level of skepticism of which our machine servants are incapable.

One could say that this is the whole reason for the creation of the cyberspace domain. People read their e-mail, visit favorite websites, even communicate through voice and video. In the context of the cyber domain we seek to use this information to achieve information superiority to make a decision faster than our adversaries. However, we know that they may be trying to leverage the cyber domain for their own purposes.

Effects that occur in this layer are changing the contents of messages to deceive the intended recipient, spoofing the source of a message, or exploiting people's trust to steal critical information. These effects are very similar to the Information Assurance (IA) skills that fall under IO. The Air Force trains end users to be wary of information and requests as well as some of the other methods of cyber attack under the umbrella of Information assurance. This is the layer to use to achieve and prevent these types of exploits.

The Skills

Now that we have a better understanding of what cyberspace is, we can begin addressing the skills required of cyber operators. The Air Force is currently using the Communications and Information Officer Career Field Education and Training Plan (CFETP) to outline the skills necessary for the old Communications and Information Career Field. With modification this will outline the skill set desired of a 17D Cyber Operator. The curriculum for the Cyber Operators Transition course (X-course) gives a good outline of what needs to be added to the existing CFETP.

Analysis of the existing CFETP along with experience completing the X-course has led to a breakout of skills required for a Cyber Operator. Comparisons with the X-course material were made with a review of the Course Training Standard (CTS) for Cyber 200, as well as the planned blocks of instruction. The course breakout of Undergraduate Cyber Training (UCT) was reviewed as well.

Organizations and Capabilities

This broad area covers the organizations that will be operating in cyberspace. This can be broken up into standard organizations and Air Force Network Operations Organizations. The standard section will address such topics as the role of A6 in component Numbered Air Forces. Air Force Network Operations covers knowledge of the NetOps command chain. This will introduce Cyber Operators to important organizations such as DISA, USSTRATCOM and USCYBERCOM, as well as the structure of the 24th Air Force to include the I-NOSCs. (AF CFETP, 2009)

Communication and Information Fundamentals

This area covers essential knowledge such as the total force concept, career field progression, roles and responsibilities of the cyber operator. This knowledge will need to be upgraded to cover the expanded skill set of a cyber operator versus a traditional communications officer. Examples would be adding targeting and mission planning to their roles and responsibilities. (AF CFETP, 2009)

Tech Fundamentals

This area will cover the bulk of the necessary skills. This is where fundamental concepts will be presented. The original CFETP breaks this area up into Communications and Computer System Fundamentals, Transmission System Principles, Maintenance Management, and Network Fundamentals. (AF CFETP, 2009) This area will need to be greatly expanded to meet the new need for greater technical skill training desired of Cyber Operators. The original CFETP defines very basic skills and concepts, and further pushes these skills into a pre-requisite module. This approach is being done away with.

The UCT course will now offer dedicated training days to cover the important network areas necessary to prepare our cyber operators. New modules will present hands on simulator training on: IP networks, telephony networks, mobile networks, satellite and space communications, and closed networks such as Integrated Air Defense Systems (IADS) networks.

The IP network area will be a major focus for the majority of operators. Not only is it the most widely used network, but many of the other networks connect to it. There are twice as many training days offered for this network then the others. (17DXX Training Transformation, 2010) This is important because IP networks follow an readily available open standard, making them relatively easy to teach. They should be presented not as the most important network, but as the best place to start learning. A solid foundation in IP networking protocols and principles will serve as an excellent springboard to learning the more advanced and specialized networks.

Telephony is an area covered in the X-Course and offered in both UCT and Cyber 200. The skills required of a cyber operator at the initial level would be knowledge of a circuit switched network, the layout of the Plain Old Telephone System (POTS), and knowledge of the DSN and red switch networks. Advanced skills would be offered in specialized Initial Qualification Training (IQT). Knowledge of mobile networks are important as well and an overview of cellular networks is desirable as well.

The study of Industrial Control Systems (ICS) is an area that does not currently exist in the original BCOT course. There are five training days allocated to this in the UCT as well as distance learning modules in the X-Course and the Cyber 200 course. Knowledge of the differing components that make up ICS such as the various control units and distributed layout of controllers and facilities is important. Understanding the systems that these networks control is important from an operational perspective as well, knowing the effects that can be achieved by targeting various elements of an ICS is important.

Space communications and control networks are covered as well, and they will present an overview of both the ground components as well as the space components that make up these networks. Important hardware and software packages such as high powered amplifiers, different types of ground antennae, and satellite control systems need to be identified.

Battlefield networks will be covered in the new curriculum as well. These will initially include sections on IADS networks and the tactical data link networks, such as Link-16. Like the other specialized networks presented in UCT through Cyber 200 as well as the X-course this will be limited to the fundamentals. Students must know the

components that make up these systems, as well as the common uses and roles of these specialized networks. Extensive hands on training on individual networks will take place in specialized IQT training courses.

Information Operations

IO skills cover the three main pillars of IO as defined by AF Doctrine These pillars are Influence Operations (IFO), Network Warfare Operations (NWO) and EW (AFDD 2-5:2-6). Material on these pillars exist in other training materials such as the Information Operations Integration Course and the Air and Space Operations Center Initial Qualification Training, both offered at Hurlburt AFB. (AF CFETP, 2009)

Cyber Operations

This area needs to address the mission planning cycle, introducing cyber operators to the Plan, Brief, Approve, Execute, and Debrief cycle. Knowledge of this cycle has not been included in previous iterations of cyber training. Targeting for desired effects and a study of effects based operations are necessary mission planning skills. These areas are covered in the X-Course as well as specified in the Cyber 200 CTS.

Cyber Law and Ethics

These skill areas will cover necessary topics dealing with applicable legal factors that affect operations in cyberspace. It is important to understand the different legal

authorities. A knowledge of U.S. Codes impacting cyber forces include: Title 10 (Armed Forces), Title 18 (Crimes and Criminal Procedure), Title 32 (National Guard), and Title 50 (War and National Defense). Important topics need to be introduced such as the Federal Wiretap Act and intelligence oversight. There is a block of instruction in all three of the new Air Force training courses.

Conclusion

This chapter presented an overview of the cyberspace environment and domain, and then presented a very broad overview of the skill sets that are recognized as being important to operation in cyberspace.

It is important to attempt to create an understandable picture of cyberspace. This is a difficult thing to do because the environment is complex and is very immature as a warfighting domain. Libicki's concept of layers provides valuable insights into defining what skills are necessary to operate in the cyberspace environment.

The skill set is also in flux, but efforts are being made to collect and consolidate them in a logical manner. This chapter outlined what the Air Force considers important, the next chapter will explain the way the Air Force is structuring its reorganization of the training pipeline.

IV: Training Plan

Just like the structure of career force the training plan to teach the necessary skills is in transition as well. Existing training is being consolidated and shuffled around to create a new pipeline for the cyber operators. A training program based on AFSPC's successful model for developing space professionals is being adopted for cyberspace professionals. This training plan has been under design for two years and is about to start its initial runs.

Concept

The desired training plan will take members from accession through senior officer ranks. The old officer training plan consisted of the college undergraduate degree, BCOT, and the Advanced Communication Officer Training (ACOT) course at the eight to ten year point. In 2007 the 39th Information Operations Squadron (IOS) launched the Undergraduate Network Warfare Training (UNWT) course to teach network warfare fundamentals. This class filled a valuable need, providing hands-on experience with simulated networks of various kinds.

These courses are being combined in the case of BCOT and UNWT. The existing ACOT course will be eliminated and in its place all 17Ds will attend Cyber 200 and 300 courses being developed at the Air Force Institute of Technology. Other courses are being injected into the training pipeline at various points to provide a smooth continuity of training and education.

Existing Training

The current training model consists of the BCOT Course at Keesler AFB. It is currently winding down operations and will become the Undergraduate Cyber Warfare Training course later this year.

This course contained a number of prerequisite materials that students were expected to complete before arriving for the six weeks of training. These prerequisite materials covered a lot of what could be considered basic knowledge about computer networks and equipment. Students received in-residence training on mobile communication equipment, communication squadron structure, some acquisition and contracting lessons, and basic electronic spectrum training.

To meet the needs of hands-on network training the 39th IOS built a comprehensive course called UNWT. This course was an overview of the major networks that the Air Force defines as critical cyberspace elements: IP Networks, ICSs, space networks, closed battlefield networks, and telephony networks. It consists of an ADL prerequisite to cover fundamentals, obtaining a civilian security certification, class room instruction, and hands-on labs incorporating simulators of each of the critical networks.

Career progression training requirements were met by the ACOT course. This was a three week class held at Keesler AFB. The target audience for this course was majors and captains selected for major. There was a large amount of reading required prior to arriving at class, consisting of materials covering all the major areas that a communication officer may have been working in prior to reaching this point in their

career. There was an exam required on the second training day on the reading material. The actual class consisted of a seminar format covering a variety of topics relevant to the career field. There was also an exercise built around a mobile communications deployment that wrapped up the course.

These courses are being phased out, and at the time of this writing they are heading into their last iterations. They are being replaced by a new training model that will combine them to ensure that students receive the necessary foundational skills at UCT. This combination of existing courses will be offered to all new accessions.

Cyber Training in 2011

The existing training will be undergoing a large transition in the coming years. The existing training courses will be completely reworked and structured into a totally new pipe line to meet training needs. New accessions entering the career field this year will be able to enter the training pipeline at the new designated entry point the UCT course at Keesler. Those who have already entered the old 33S career field, and those coming from existing career fields will have a few options available to them.

The UCT course will begin in 2010. It will consist of a program incorporating some of the old BCOT training, as well as the material from the 39th IOS's UNWT course. Students will be placed into one of two career shreds after graduating from UCT. The "A" shred will be Cyberspace Warfare Officers responsible for planning, organizing and performing active network defense, exploitation and attack in support of joint, national and AF objectives. The "B" shred will become Cyberspace Control officers who

will be responsible for planning organizing and performing Net Ops to include establishment and passive defense in support of joint, national, and AF objectives. (Air Force Roadmap, 2009) The expected split coming out of UCT is 20% A shred to 80% B shred.

The "A" shred students will go on to attend the Intermediate Network Warfare Training (INWT) course at the 39th IOS. This course is meant to provide a higher level of learning than the original UNWT course. "B" shreds will continue on to their unit for Initial Qualification Training required for their particular job.

Further training will take place with the Cyber 200 and Cyber 300 courses being offered at AFIT starting in June 2010. These courses replace the ACOT class. The Cyber 200 class will be available for captains, which is earlier than a communications officer would expect to attend ACOT. This course will offer lectures and hands-on laboratory sessions and provide a more interactive experience than the old ACOT course.

Cyber 300 will be a further offering for senior majors, also being prepared by AFIT for the June 2010 timeframe. This will be a shorter two-week class designed to prepare students for the larger issues facing the cyber operator career field. It will be a discussion format course and provide the opportunity to discuss issues such as policy, doctrine, roles and responsibilities, response thresholds, etc.

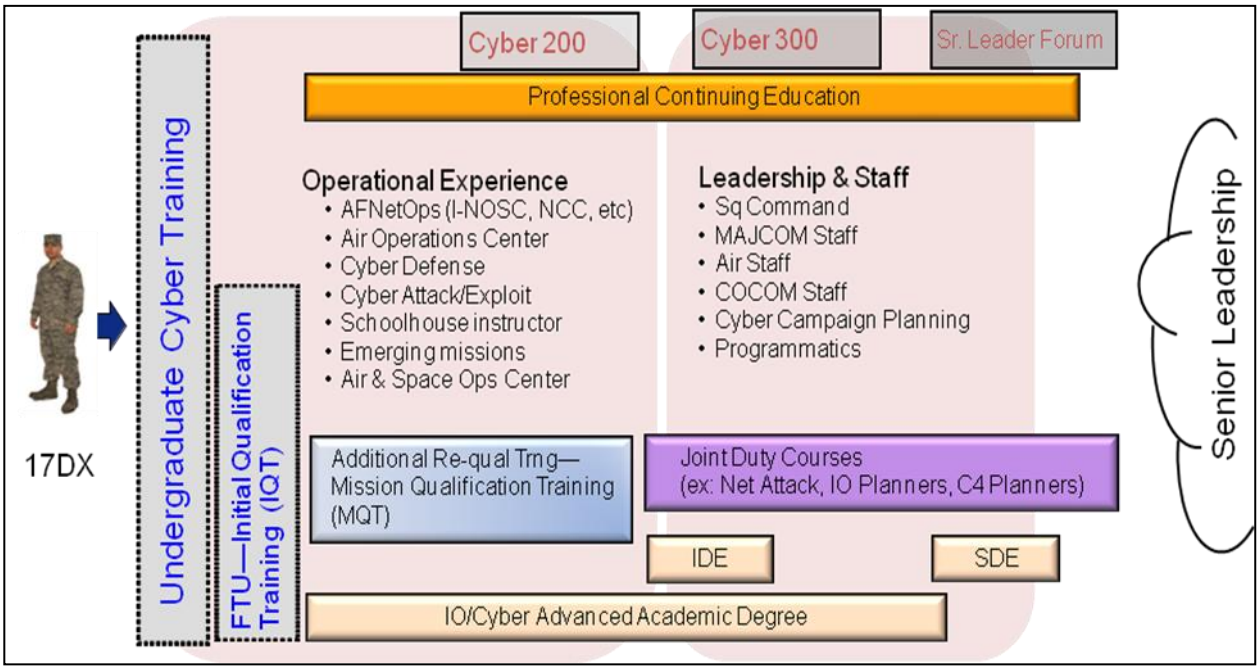

Figure 2. Training Path (17DXX Training Transformation, 2010)

Transition Course

To handle the transition from Communications officers to Cyber operators the Air Force is offering a transition path so existing captains and majors can wear their Cyber Operator badges. This transition course has come to be known by its informal name "X-Course", and it contains a large amount of information delivered in an ADL course. It is designed to take approximately 40 hours to complete. It covers a large amount of material that will familiarize communication officers with material they would have received in the newer UCT and UNWT courses. (Cyber Operations Transition Course, 2009)

Areas covered by the X-Course include information on the structure of the 24th Air Force and supporting organizations across the government to include research labs

and support agencies. Technical information is included about the networks the Air Force considers critical to the cyber domain. These include telephony, IP, ICS, space networks, and closed battlefield networks. Legal issues concerning cyberspace are covered as well. Vulnerabilities and mitigation techniques for all of the critical networks are covered. The course ends with a series of scenarios that illustrates the concepts taught. (Cyber Operations Transition Course, 2009)

Students are required to complete the course work within a one month time period. Progress is measured by a sequence of tests after every lesson. Students must score an 85% on each test, and those students receiving a lower grade are allowed two retests. The lessons are roughly the same length long, with a few being quite long and detailed.

This material is very close to what is offered for the UNWT course at the 39 IOS, in fact if a student has participated in the UNWT course their completion certificate will count for qualification for wear of the Cyber Badge. The X-course is designed to be available for students to use for a one year period. This will allow majors and captains time to take this course and be eligible to wear the new cyberspace badge at a level appropriate to their current 33S skill level.

V: Gaps/Issues

At present the Air Force is transitioning from a training model designed for communications officers to one providing training and education for cyber operators. The new training is more focused on various networks that cyber operators will be required to work on. There is more emphasis on providing hands-on experiences at an earlier point in training. For the next several years there will be a number of issues to address. Some of the problems that will arise in this upcoming transition for officer training and education can be identified.

There continues to be a lack of a strong prerequisite for those entering the field. A stronger skill categorization system could reduce repetition across different classes and ensure the proper skill levels are taught at the appropriate points in training. The reliance to push large amount of training to ADL must be tempered to match the training objectives with the strengths of ADL.

Skill Categorization

There are many broad areas of skills in the cyber career field. Communications officers tended to be proficient in the various areas that they have worked in during their career. Senior communication officers have skills that range from acquisitions, executive officers, network operations and even visual arts.

The different certifications and methods for keeping skills current in the technical aspects are a necessity of the rapid pace of change in the curriculum. The Air Force is

having a difficult time keeping courses current because the rate of change in technology is faster than the current method for creating, updating and validating and creating course content.

The current method of developing courseware in the Air Force is known as the Instructional Systems Development (ISD) process.

> Since 1965 the Air Force has used the Instructional System Development (ISD) process to help commanders and managers resolve the instructional dilemma. ISD is a flexible, proven process for determining whether instruction is necessary in a given situation, for defining what instruction is needed, and for ensuring development of effective cost-efficient instruction. (Air Force Handbook 36-2235)

This system has served the Air Force well, and it provides a flexible iterative process for creating and managing courseware. The problem is that in the 21st century it may not be flexible enough. The system does not need a total overhaul but could benefit from small changes.

One shortcoming is in the analysis phase a list of broad knowledge areas is broken down to specific tasks. This leads to line item tasks that are extremely vague and open to interpretation. One example that shows up frequently among many course design documents is the desire for the student to learn and retain facts about the electromagnetic spectrum. The task item placed on a training task list states electromagnetic spectrum. A course developer has little more to go on. They need further information such as: Can I assume any prior knowledge of basic physics, how much math can I expect my students to understand? Will they ever build on this knowledge again so I know where to bound my lesson?

Right now the only factor given is the level of learning against which the lesson is developed. The current breakout for knowledge levels are in the table below.

Table 1. Proficiency Codes

Scale Value	Proficiency Code
A	Can identify basic facts and terms about the subject. (Facts)
B	Can identify relationship of basic facts and state general principles about the subject. (Principles)
C	Can analyze facts and principles and draw conclusions about the subject. (Analysis)
D	Can evaluate conditions and make proper decisions about the subject. (Evaluation)

We need better criteria for labeling our desired skills to fit in with the highly modular education and training model that is being developed for our cyber forces if we are to keep up with the rapid rate of curriculum change.

Standardizing Entry Qualifications

Entry level qualification needs to be tightened up for the cyber career field. The current entry criteria is

> Undergraduate academic degrees in at least one of the following disciplines; computer science, cyberspace studies, information management, mathematics, engineering, physics, or business disciplines with information management, or computer science specialization.

> Officers not meeting academic degree requirements can have a minimum of 24 credit hours of Information Technology related courses; to include but not limited to courses in telecommunications, computer science, upper-level mathematics (200 level or higher), engineering, physics, information systems management and information resources management. Graduate academic degrees in the above disciplines will also be considered. (AF CFETP, 2009)

There are a few problems with these requirements. Colleges and universities have different programs and emphasis areas. A computer science class from one school is not necessarily equal to one from a dedicated technical school. A definition of cyberspace studies is difficult to find, however there are many studies on the impact of cyberspace on traditional non-technological subject areas such as cyberspace and psychology, cyberspace and sociology and cyberspace and economics. An officer with one of the stated degrees could most likely achieve success in the career field, but one meeting the 24 credit hour requirement introduces some problems.

This problem poses some difficulties. One idea is to do away with the credit restriction and only allow people with technical degrees to enter the career field. This is not a feasible solution because the number of people with these degrees is not adequate to meet the manning requirements of the career field. A solution to mitigate this shortfall is to take advantage of opportunities available with a new training program. The Air Force must take great efforts to ensure that in this iteration of the training program the UCT class provides all officers with a solid foundational baseline to build upon in further training.

Use of Advanced Distributed Learning

ADL is a concept that has taken off over the last decade. It is an advancement and improvement to Computer Based Training. ADL adds a layer of administration and management to the student's experience.

In traditional Computer Based Training (CBT) students would access content, read through it, possibly take an exam, and then register that they have completed the training. These courses were offered to supplement lengthy annual training and simple introductory training.

The concept of ADL builds on this by incorporating a curriculum management system to control who has access to the course, track progress through the course, and assist students in their progress. The courses can be monitored by properly trained instructors who can assist students as well as validate course completion. They are also able to help with frustration of dropped registrations and lost and forgotten passwords.

In residence course time is able to be reduced, in some cases up to 3 weeks. This has many benefits to the Air Force. Travel costs are reduced as the number of weeks of TDY is cut. Introductory materials are often converted to ADL lessons and can cut off the first few weeks of training, allowing the students to arrive with a base level of knowledge that the in-residence instructor can rely on. The ADL can be monitored and those not finishing can have their order cut and they will be disallowed from attending. This frees up staff time as well, with this time being available to work on course improvements, administrative necessities and time for leave. This is necessitated because

the throughput for courses is growing and growing and a most likely use for the freed up time is to insert more courses into the gap.

Money is saved is as well as the cost of printed material is reduced. Most ADL curriculum consists of web pages, web animation (such as Adobe Flash content), converted PowerPoint presentations, and printable Adobe Portable Document Format files. As technology advances, more and more digital formats become available; for example it is not uncommon to be able to download recorded audio from a lecture to listen to during a commute (e.g., Podcasting).

Workers are able to take advantage in the freedom of schedule that ADL provides. These courses can be taken on the student's schedule, and at the student's choice of location considering technical requirements are met. Whether or not the home installation allows students a few hours a day to complete prerequisites is up to individual commanders and mission requirements, however most would rather have the people on station for an additional three weeks than have them out of the office entirely. ADL offers one other benefit over traditional CBTs and that is the presence of an instructor to keep students on track. It is ultimately each student's responsibility to complete their training, however some course are monitored and students not making sufficient progress are notified and reminded of the schedule for completion. This drastically cuts down on the number of students who fail to complete their training.

Although ADL can bring many cost savings, it does have drawbacks. Despite the involvement of instructors and facilitators students still feel isolation and a sense of them versus the technology. Keeping students in the workplace often means they have the same high commitment to work and cannot get away from the work center. Technology

can sometimes be a roadblock as well as an enabler, and security restrictions may prevent the student from working on the ADL class at home.

Training mismatch between junior and mid-level officers

When the change comes to create a new training pipeline there will exist a difference in the training and education experiences between junior and mid-level officers. Junior officers will have had the benefit of the new updated courses for cyber operators. They will benefit from being brought up in the operator focused training and will have more hands on experience than the officers who graduated from the old BCOT course in the previous three years.

Mid-career officers would ideally be getting ready to enter the ACOT course. These officers will instead be placed into the Cyber 200 and 300 courses. These students cannot be expected to have the ideal level of training that those new 17Ds will receive coming fresh into the new training pipeline. For the next few years a compromise must be found to ensure when they leave Cyber 200 they have the same training opportunities that the newer 17Ds will have.

Officers entering these courses will not have the basic level and knowledge that the courses are being designed for. For this purpose the classes will focus on a mix of briefs and hands-on labs. The training days will be long to be able to incorporate all the required training, as well as to be able to maintain course throughput. This is probably the best solution for now, but ideally as more technically experienced new 17Ds enter

into the Cyber 200 course the curriculum will have to be modified to reduce repetition, and the training day can become more modest.

The students who will be outside the pipeline for Cyber 200 will be entered in Cyber 300 and may very well miss out on any technical hands on experience. This has the potential to make it hard for some of the less technical to communicate effectively with the younger officers. This factor is mitigated because at the senior level of their career most of these officers have demonstrated the skill to be generalists and have made it this far with a form of training that worked for them so this sub-issue will be a small one.

Conclusion

There always have been and probably always will be training gaps in the communication career field. Many of these gaps can be overcome, and institutionally, the Air Force has a chance to correct some of the problems that have plagued us in the past. Care must be taken to ensure that the effects differing levels of training experience are minimized. We may take this opportunity to properly categorize our skills. Proper use of ADL Assets can provide a means of filling some of our gaps. There are many ways to mitigate these issues that will be explored in the following chapter.

VI: Closing the Gaps

Overview

The effort to redefine the training path for cyber operators is under way. The challenge is to move from the current model to a training plan that provides more focus on the many different types of networks that cyber operators will work on, as well as covering the hands-on skills the new force will require. This will be a difficult task, and this chapter will present some ideas for closer coordination between the different schoolhouses as the new training program takes shape.

This chapter will offer some ideas to mitigate the concerns raised in the previous chapter. It will offer suggestions for different methods for organizing the required skills, and best practices for incorporating ADL into existing curriculum.

Reorganizing the skill set

There is a great deal of duplication of effort in training across the different courses under development. Each class is supposed to ensure that it builds on the material that comes before it, but care must be taken as all these courses are in a state of revision and consolidation.

The skills discussed in the previous chapter can be organized many different ways. It is valuable to be able to look at these skills along many different axes of where they belong in regards to point in career, whether it is considered a foundational skill or if it should build on skills that should have been delivered in a previous course.

The required skills can be placed in a table categorizing them separately according to the factors: Operational or Technical, Cyber Layer, and Career Progression. By using a tool like this we can properly tailor our training as to what types of education needs to be delivered at each phase of training as needed with a minimum of duplication.

To meet the specific military needs in cyberspace skills can begin to be categorized and assigned a proper place in the training continuum. There are many different categories in which to place these skills:

Technical: Relating to the technical aspects of the career field

Operational: Relating to the operational aspects of the career field

Cyber Skills: Existing at a certain layer of cyberspace

Physical Layer

Semantic Layer

Syntactic Layer

Sequence: Where training logically belongs in relation to other skills

Foundation - Skills required for all members, may be built upon

Follow on - Builds upon foundation skills for members requiring them

New Technology - Skills required for new tech that emerges

Career Progression: Skills and knowledge desirable for certain levels

UCT

Professional Development (200, 300 level)

These categories represent groupings of different factors, such as time in grade, training required upon joining a new unit, training required when changing career fields, training required to stay current with the technology of the career field. Different factors

can be assigned to the same skill for example the skill “Social Engineering” could be tagged with being a technical skill, existing in the physical layer of cyberspace, to be taught at a foundational level, and delivered at the undergraduate level. Further applications of this skill will be taught at individual unit training programs if it is required for that unit’s mission. An example of classifying a progression of skills using these categories can be found in Appendix 1. These classifications could be a valuable tool for use by the schoolhouses when designing curriculum.

Leveraging Advanced Distributed Learning

ADL provides great benefits to both the student and the learning institution. There are drawbacks as well, and care must be taken not to push too much into the advanced distributed learning portion of any class. ADL is not a panacea, and there are a number of best practices to be followed. These include the length of a lesson, maintaining consistent difficulty within a course, and the need for technical support for students.

Lesson length

Do not put too much into each block. Students will be taking this either at home or in down time at their home station. They need to be able to reliably budget time to participate in the course and benefit from the training. Overly long lessons, or lessons that are of inconsistent length make it difficult for the students to plan their schedules.

The ability to save progress mid-lesson helps, but a student who is able to complete a tangible section of learning in a single time session is going to enjoy their learning more.

Difficulty

Consistent difficulty in objectives across lesson within a single course is important as well. A student gets frustrated when one block has definitions clearly spelled out and the next asks a question requiring them to pick out a minor item buried in a long list. It is important to call attention to required knowledge, like a live instructor emphasizing important points of a lecture.

It is very difficult to incorporate levels of learning above the B level into ADL lessons. Most ADL course use a multiple choice test as a method for evaluation and these are poorly suited to test higher levels of learning. Some lessons are able to incorporate longer assignments such as essays submitted online and graded by an instructor. This is an acceptable solution to attempt to meet higher learning objectives, but you lose the ability to provide the student with instant feedback on their status.

Technical Support for Students

It is important to provide as much technical support as possible behind an organization's ADL products. Recognizing the fact that ADL lets students stay in the workplace longer comes with the fact that they will still have work center related issues to face and their online course work will most likely be lower in priority than day to day

emergencies. Students will not want to be fighting technical issues when trying to fit their ADL learning into a busy day. A single point of contact for technical support goes a long way to letting them feel like they are accomplishing necessary training that is important rather than an afterthought pasted onto an in-residence course.

Because of the need to offer live support for these classes the course size should be kept small as well. Often the ADL component of training is seen as a construct that you can pump as many students through very quickly. When course sizes are kept small instructors are able to be more responsive to student needs.

By following these guidelines ADL can be successfully incorporated into the training path. It is best used to reinforce existing in-residence courses rather than a means to funnel more students through a faster, cheaper training substitute.

VII: Conclusion

Background

The purpose of this Graduate Research Project is to examine training efforts through the years following the transition of Communications Officers to Cyber Operators. This paper looked at the decisions that the Air Force took to bring us to the current state of the career field. A brief look at the cyber environment and domain and a summary of the necessary skill set was presented. This was followed by a look at the old training model and an explanation of the new courses coming out in 2010. Finally some potential problem areas were raised along with some proposed solutions.

The Air Force has taken a big step in changing the old communications career field to force of cyber operators. In a time where the DoD is defining the cyber environment and domain the Air Force is preparing itself to have well-trained force of operators to meet whatever challenges may await them. Many of the skill are known, indeed many have been taught in the old training model. Some fall under new areas that have been recognized as critical as our knowledge of the environment matures, and some are unknown and will need to be incorporated as new technologies and threats emerge.

Recommendations

In this time of change there are some opportunities for improvement. Great steps have been made to improve the training programs, especially in the technical areas. In the years that follow there is great opportunity to ensure that the new training program

not only meets the Air Force's needs, but improves on what preceded it. This paper recommends taking the following steps:

> Close monitoring of UCT graduates will ensure that they have a solid baseline of training that can be built upon in the follow-up courses.
>
> Improved classification levels of desired skill can be shared by the various schoolhouses to reduce repetition and aid in the course development process.
>
> Judicious use of ADL techniques can both save money and provide a valuable experience when combined with in-residence training.

The Air Force is ready to take on the challenge of entering the cyber domain. There is still much to learn about this evolving domain. With every major change unique opportunities present themselves, and this transition is no different. The Air Force should be aware of and take advantage of these to ensure its force of cyber operators is able to dominate cyberspace in the same manner it does Air and Space.

Appendix 1

This Appendix presents an example of how to classify a sequence of skills using the categories explained in chapter 6. It shows a sequence of skills related to IP networking. This is meant to show how the designators progress through the various levels as the tasks get more specialized, as well as incorporating some of the higher level operational concepts.

This example specifically deals with learning how to manually craft packets to defeat an Intrusion Detection System (IDS). It shows how at the foundational level a student needs to know how to read hex and binary, this is to ensure they can read a packet diagram. Foundational level lessons will cover reading diagrams, and identification of key fields in an IP packet.

The follow on skills necessary build on foundation to teach the more focused task of bypassing an IDS. The concept of packet fragmentation would be covered, explaining how various pieces of hardware fragment packets and the reasons for doing so. The art of manually crafting packets is follow on knowledge building on the students prior knowledge of now packets are constructed. Finally the application of using manually created packets to bypass intrusion detection systems completes the technical learning required to understand and perform this task.

Examples of potential operational skills required to gain a more complete picture for military application of these skills follow. Theses example include NS factors that need to be considered when attempting to penetrate an IDS. These items would include briefs on different IDSs, availability of different IDS and potential adversary use of IDSs.

A higher level operational case study lesson would be appropriate for the 300 level where discussion of historical successful penetrations (from friendly and hostile perspectives) can be explored.

This tool is presented to show one potential use of more detailed categorization criteria for cyber skills. By using this or a similar system schoolhouses can create a more robust language for defining what they are required to train, creating a better fit between different levels of training.

Table 2: Sample Skill Categorization

Skill	Type	Cyber Layer	Sequence	Career
Hex/Binary	Technical	Syntactic	Foundation	UCT
Reading Packet Diagrams	Technical	Syntactic	Foundation	UCT
Identify Key Fields	Technical	Syntactic	Foundation	UCT
Fragmentation	Technical	Syntactic	Follow-on	200
Manually crafting IP packets	Technical	Syntactic	Follow-on	200
Manually fragmenting IP packets	Technical	Syntactic	Follow-on	200
Using fragmentation to bypass Intrusion Detection Systems (IDS)	Technical	Syntactic	Follow-on	200
Network Support considerations for bypassing IDSs	Operational	Syntactic	Follow-on	200
Case studies of infiltration of IDS	Operational	Syntactic	Follow-on	300

BIBLIOGRAPHY

Department of the Air Force. *AFSC 33S Communications and Information Officer Career Field Education and Training Plan (AF CFETP),* November 2009.

Department of the Air Force. *Managing Advanced Distributed Learning (ADL).* AFI 36-2201 Vol 4, October 2002.

Department of the Air Force. *Information for Designers of Instructional Systems - ISD Executive Summary for Commanders and Managers.* AFI 36-2235 Vol 1, September 2002.

Department of the Air Force. *Air Force Doctrine Document 2-5, Information Operations,* January 2005.

Department of the Air Force, SAF/XCTF. "17DXX Training Transformation". February, 2010.

Department of the Air Force, Air Force Institute of Technology. Cyberspace 200 Course Training Standard, 2009.

Department of the Air Force, 229 IOS. *Cyber Operations Transition Course.* November, 2009, https://cyber.iovermont.org.

Department of the Air Force, *The Air Force Roadmap for the Development of Cyberspace Professionals 2008-2018 (Change 1)-Draft,* 2009.

Department of the Air Force, *Air Force Doctrine Document 3-12, Cyberspace Operations-Draft.* DoD:Washington, March 2010

Department of Defense. *National Military Strategy for Cyberspace Operations (NMS-CO).* Version 6.0. Washington:DoD. 25 August 2006.

Franz, Timothy P. *IO Foundations to Cyberspace Operations: Analysis, Implementations Concept, and Way-Ahead for Network Warfare Forces.* AFIT/GIA/ENG/07-02. MS Thesis, Air Force Institute of Technology(AU), Wright Patterson AFB OH, March 2007.

Libicki, Martin C. *Conquest in Cyberspace.* New York: Cambridge University Press, 2007

Pampe, Carla. "Air Force activates cyber Numbered Air Force" (August, 2009), accessed 3 Jun 2010, http://www.afspc.af.mil/news/story.asp?id=123163863

Rattray, Gregory J. "An Environmental Approach to Understanding Cyberpower" in *Cyberpower and National Security.* Ed. Franklin D. Kramer. Dulles VA: Potomac Books, 2009.

Shachtman, Noah. "Air Force Suspends Controversial Cyber Command" *Wired,* (August 2008), accessed 3 Jun 2010, http://wired.com/dangerroom/2008/08/air-force-suspe/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
10-06-2010	**Graduate Research Project**	Jun 2009-Jun 2010

4. TITLE AND SUBTITLE

Managing Cyber Operator Training Curriculum

5a. CONTRACT NUMBER

5.

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Beach, Matthew G., Maj, USAF

5d. PROJECT NUMBER

7.

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ICW/ENG/10-01

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

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

The purpose of this research was to examine the state of various training programs existing for communications officers, and new training being developed for the new 17D cyber operator career field. The methodology for this project consisted of a review of existing training plans for communications officers, a review of course design documentation for new course development efforts, a review of the new career training plan, and a review of the content of the 33S to 17D transition course (X-Course). These materials were reviewed and potential problem areas were identified.

15. SUBJECT TERMS
Cyber Operators, Training

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Mills, Robert J.
U	**U**	**UU**	**UU**	54	**19b. TELEPHONE NUMBER** *(Include area code)* 3636 x-4527 robert.mills@afit.edu