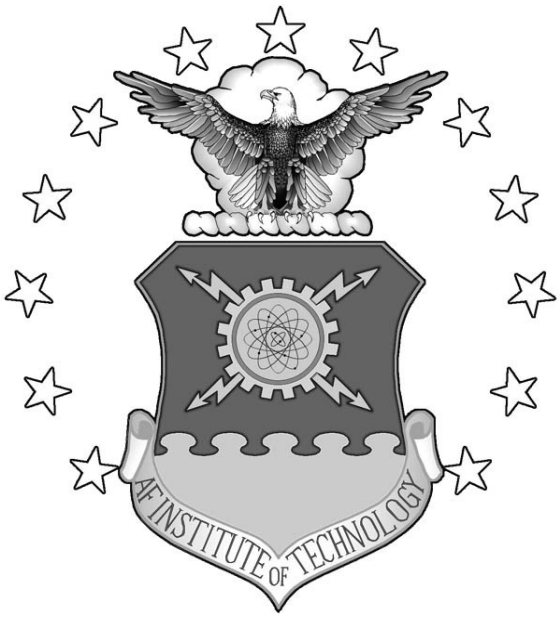
3-22-2007

In Pursuit of an Aptitude Test for Potential Cyberspace Warriors

Tiffiny S. Smith



IN PURSUIT OF AN APTITUDE TEST FOR POTENTIAL CYBERSPACE WARRIORS

THESIS

Tiffiny S. Smith, Captain, USAF

AFIT/GIR/ENG/07-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GIR/ENG/07-01

IN PURSUIT OF AN APTITUDE TEST FOR POTENTIAL CYBERSPACE WARRIORS

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

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 Master of Science in Information Resource Management

Tiffiny S. Smith, BS

Captain, USAF

March 2007

AFIT/GIR/ENG/07-01

IN PURSUIT OF AN APTITUDE TEST FOR POTENTIAL CYBERSPACE WARRIORS

Tiffiny S. Smith, BS

Captain, USAF

Approved:

_____/signed/_____	14 Mar 2007
Dr. Robert F. Mills (Chairman)	date
_____/signed/_____	16 Mar 2007
Dr. Dennis D. Strouble (Member)	date
_____/signed/_____	14 Mar 2007
Dr. Michael R. Grimilia (Member)	date

AFIT/GIR/ENG/07-01

Abstract

The Air Force has officially assumed the cyberspace mission. In order to perform the mission to the best extent possible, it is important to employ personnel with the necessary skill sets and motivation to work in this type of environment. The first step in employing the right people is to screen all possible candidates and select those with an aptitude for acquiring the skill sets and the motivation to perform this work. This thesis is an attempt to determine the necessary skills and motivations to perform this work and recommend a screening process to select the candidates with the highest probability for success. Since this mission is new, determining what skills and motivations are necessary is difficult. To assist in determining the skills and motivations for cyber warriors, this thesis considers the skills and motivations of computer hackers. If the skills and motivations of successful hackers can be identified, those skills and motivations can be used as a tool for developing an aptitude test to be used as a screening device. Aptitude tests have proven to be a valuable resource to the military and academia. A blueprint for an aptitude test is provided based on the findings of the hacker skills and motivations.

Table of Contents

List of Figures

Figure Page

List of Tables

IN PURSUIT OF AN APTITUDE TEST FOR POTENTIAL CYBERSPACE WARRIORS

I. Introduction

1.1 Background

On Dec 7, 2005, Air Force leaders released a new mission statement, "to deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in Air, Space, and Cyberspace" (Wynne & Moseley, 2005). This was the formal acknowledgement of cyberspace as a domain in which the military can and will wage war. As with the adoption of any new mission, this brings some challenges. One of the challenges is the determination of who should be selected for training and education as a cyberspace warrior. The challenges regarding the selection of those individuals are the specific problem addressed here.

> A fundamental problem in personnel selection is to choose from a large group of job applicants, from which a smaller group is to be employed. The goal of personnel selection is to designate the individuals who should be hired. These individuals are chosen because the selection techniques predict that they can best perform the job in question. (Gatewood & Feild, 2001)

When screening and hiring job applicants, there are four possible outcomes:

1. The *right* person is hired
    - The individual works well in the organization, advances it, and contributes significantly to the mission
    - Best possible outcome for individual and organization
    - Successful screening process

2. The *wrong* person is not hired
    - Eliminated someone with a potential to hinder operations
    - Positive outcome for the organization
    - Successful screening process
3. The *wrong* person is hired
    - Individual that lacks qualifications, motivations, or experience or does not fit in and degrades the mission
    - Negative impacts to the organization may include, but are not limited to: added time for training, dependence on others for task completion, or inability to work with others
    - Unsuccessful screening process
4. The *right* person is not hired
    - Individual with qualifications, experience and potential to contribute to the mission is not hired
    - Individual works for the competitor, or adversary, and contributes to their mission which is a threat to the friendly mission
    - Unsuccessful screening process

"Our enemies may well be training their soldiers in the art of cyber warfare to attack our infrastructure and defend their own. It seems like a no-brainer that these groups would also recruit knowledgeable hackers from anywhere in the world for training and for mission-critical projects" (Mitnick & Simon, 2005). In the case of cyber operations, the latter two outcomes could be a tragic mistake. If the Air Force is unable to weed out the right people from the wrong, then cyber operations could suffer dramatically. If,

however, the Air Force is able to implement a process that consistently identifies the right people, cyber operations will likely be very successful even as the mission morphs as it searches for its place in the Air Force.

The ultimate goal of this research effort is to develop a valid and reliable screening process that serves as a filter for separating individuals with a high probability of success as a cyberspace warrior from other candidates. The format of the filtering process may be a combination of tests or a set of questions to supplement existing tests, interviews, situational exercises, any combination of these, or some way that has not yet been determined. No matter what the format, the method implemented should obtain the goal of the screening process. The recommended filtering process includes variations depending on many factors. Some of these factors include consideration of the candidate's stage in his/her career (i.e. potential enlisted recruit vs. current military member), the candidate's education, training and experiences, the candidate's motivations, and his/her ability to thrive in such an environment. All these testing concerns will be addressed to some degree in this thesis. The recommended composition of the screening method will be in Chapter IV of this document. The method will be designed to assist the Department of Defense (DoD), and specifically the Air Force, in its selection of cyberspace warriors. This thesis lays the foundation upon which to meet that ultimate goal. Although tests are not provided here, creation of tests and other screening methods, based on the findings of this research, are the logical next step. Suggestions for these will be elaborated on further in Chapter V.

The government believes in testing all recruits and attempting to place them in jobs for which they have an aptitude. This belief is demonstrated by the mandated use of

the ASVAB for all services in 1976 and the Air Force's use of the AFOQT since 1957 (Carretta, 2000; Davidson, 2005) (respectively). As cyberspace is a new part of the mission, it is logical that a new aptitude test be developed to ensure those with the special abilities or skills are selected for these positions and especially to make sure those without the aptitude are excluded from such positions. The hiring and not hiring of the right person is critical for cyberspace operations since they have the potential to devastate an adversary politically, publicly, morally, financially and in all aspects. Because of the power associated with these operations, the people hired must have the right experience, skills, abilities, knowledge, and especially the right motivations. Skills, knowledge, and ability are relatively easy to test, but motivation is more difficult.

Before a test can be developed, many decisions must be made regarding the content, the length, and the format of the test. Other concerns include determining who will write the test, where and when it will be given, to whom it will be given, what scores are acceptable, and what is the training and career path or options for those that demonstrate an aptitude and motivation for work as a cyberspace warrior. Some of these concerns will be addressed in this work while others are acknowledged but left for others to address. There is one known existing test designed for candidates in a cyberspace role. That test will be reviewed and critiqued. Although neither that test nor the recommendations proposed will be the definitive work on this subject, this work should initiate conversations, debates, tests and studies in this area that will lead to the development of a screening process and tests.

The first step in developing a selection measure is "Analyzing the job for which a measure is being developed" (Gatewood & Feild, 2001). This is a challenge for an

emerging field as there is no job to analyze. Therefore, identifying a group of people who appear to be performing the desired job can be analyzed. In this case, computer hackers appear to be that group. "Experts agree knowing more about the different skills, personality traits and methods of operation of computer criminals could help the folks pursuing these criminals" (Bednarz, 2004). Until now, the desire to understand hackers was to defend against them:

> In order to better understand how computer attacks are conducted, it is very important to gain insight into what drives people to do those attacks. This will allow us to understand the way they work, their community, motives, etc., which will then enable us to protect our systems in a more efficient way. (Arief & Besnard, 2003)

However, this research applies our understanding of hackers not as a way to defend against them, but as a way to identify and recruit cyber warriors with the same skills and motivations that make computer hackers so good at what they do.

1.2 Problem Statement

The growing importance and possible ramifications of cyber operations compel the Air Force to have the *right* people in these positions. The filtering method proposed here is a testing process. This testing process would serve as a method to separate those who are likely to be successful from those who are unlikely to be successful in conducting such operations. In the absence of an existing test, observing the skills believed to be necessary to be successful can be used to devise a test based on those skills. In this case, the hacker community represents people who have the skills the Air

Force cyber force needs. Therefore, observing hackers to determine what makes them successful, should aid in the recognition of skills that should be assessed and measured.

Based on the background provided, the following is the problem that is addressed in this thesis: Cyberspace operations are a part of an advancing domain in the military war-fighting arsenal that requires the selection of appropriate personnel. To select these individuals, a screening process must be devised to ensure those with the highest probability for successes in this domain are selected for such positions and/or additional training and education. This research is intended to address this problem by way of a proposed solution, as follows: There are certain traits, characteristics, skills, knowledge, and motivations that an individual with an aptitude for cyber operations poses. If the aptitudes and motivations can be identified then they can be quantified and tested. Computer hackers provide a group of individuals that poses the skills and motivations the Air Force desires for cyberspace warriors. Analyzing them will provide a way to identify and thus test for and measure the desired skills and motivations needed for cyberspace warriors. The identified skills and motivations can be used to develop tests and/or methods to screen potential cyberspace warriors. These tests and methods can be used to filter candidates with the highest likelihood for success in cyberspace operations.

A screening process, such as the one proposed here is actually another take-away from the hacker community. Rosteck notes that owners of hacker bulletin boards screen their candidates just as this thesis proposes the military do for its cyberspace warriors. "Such tests serve as filters for worthy and un-worthy potential new members; it is imperative that new users be screened properly" (Rosteck, 1994). These tests may be questionnaires with technical questions or the prospective member must complete a hack

and prove he/she has the skills and knowledge to hack and will add to the knowledge on the bulletin board.

1.3 Key Terms

There are many terms in this paper that require clarification. Some of the words have multiple meanings while others are relatively new, others still are somewhat unique to this area of study, and some are dominant in military jargon. This section is devoted to explaining how these terms will be used in this paper.

A key component of a cyberspace warrior is cyberspace. The Joint Chiefs of Staff defined 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" (Kass, 2006). As already noted, this paper will focus on the networked systems and associated physical infrastructure as a method for war fighting. Unless otherwise specified, the terms cyberspace warrior and cyber force refer to those that attack, exploit, survey, research, and plan military operations taking place in computer networks and associated hardware, software, applications, infrastructure, and architecture.

Another recurring and important term throughout this document is hacker. Originally, the term hacker was considered a compliment. "It used to be a compliment; then it became an insult" (Schneier, 2000). Now, the same term provokes thoughts of mischief and mayhem. Nissenbaum suggests two possible reasons for the shifts in the perception of hackers. She suggests that one possibility is that hackers have changed

from doing work for the greater good to not caring who their victims are. Her second suggestion is that society has changed standards and values and now society sees hacker activities as wrong. (Nissenbaum, 2004) Other terms are newbies, crackers, hacktivits, and cyber terrorists.

According to dictionary.com, a computer hacker is defined as:

1. One who is proficient at using or programming a computer; a computer buff.
2. One who uses programming skills to gain illegal access to a computer network or file.

(Hacker, 2007)

Although these two definitions are the crux of the definition, there are some hackers who are not programmers. These hackers have been classified as newbie/tool kit (NT).

> The NT category includes those persons who have limited computer and programming skills. These persons are new to hacking and rely on already written pieces of software, referred to as tool kits, to conduct their attacks. The tool kits are readily available on the Internet. (Rogers, 2003a)

For purposes here, the term hacker does not signify a category of certain skill level. Nor does the term indicate, as many hackers suggest, someone who uses his/her skills to help society. Many hackers claim, "that although they have the ability and the means to cause harm, it was neither their intention nor their practice" (Turgeman-Goldschmidt, 2005). For the purposes of this research, there is no discrimination between terms or categories. The military cares little about what category a person or group holds when defending the network. Any person who uses a computer or its resources without proper authorization is considered a hacker, regardless of their intent, motivation, or skill level. Furthermore,

for the purposes here, all the skills and motivations of all these people are useful to the Air Force as hackers provide the basis for a selection method.

The third key term in this thesis is aptitude. Dictionary.com provides the following definitions:

1. An inherent ability, as for learning; a talent.
2. Quickness in learning and understanding; intelligence.
3. The condition or quality of being suitable; appropriateness.

(Aptitude, 2007)

These definitions provide an acceptable description of the term with one enhancement. Here, aptitude refers to not only an ability to learn or talent, but also the desire to learn or use the ability or talent.

The final term that needs to be defined is motivation. Although typically understood, since it is one of the main points of the research, it is important to be clear on how the word is used. Wordnet's first definition accurately describes the meaning used here: the psychological feature that arouses an organism to action toward a desired goal; the reason for the action; that which gives purpose and direction to behavior. (Motivation, 2007)

1.4 Limitations

One limitation of any thesis is the time limit. This thesis was completed during an 18-month program in Information Resource Management at the Air Force Institute of Technology. Many of the classes, projects and papers required throughout the program contributed to the research and knowledge used to develop this document. However,

most of the writing and specific research was accomplished during the final four months of the program.

Another limitation is the lack available knowledge or experts within the Air Force. As already noted, cyber operations are new to the Air Force and although much work is in progress, few decisions or actions are completed. Since the experts within the Air Force are still undetermined, it was necessary to extrapolate who the experts will likely be and what type of work the cyber force will probably be doing from available briefings, documents, conferences, meetings and other similar resources. The references available within the military are drawn from closely related subjects, predominantly communications and information and intelligence.

Another limitation encountered for this thesis is the lack of previous research or writings on this topic in the civilian and academic settings. When speaking about research regarding cyber terrorists, Schudel, Wood, and Parks state "Very little intelligence or other data exist in open literature that characterized the behavior or existence of this class of adversary" (Schudel, Wood, & Parks, 1999). Again, it is an emerging discipline, which necessitates that research be assembled from related fields and/or areas of study. The premise here is that the military should consider what skills and motivations hackers have because they personify, to some degree, the skills, and motivations the Air Force needs in a cyberspace force. However, it is difficult to find many scholarly writings on hackers and their skills, traits, abilities and motivations. It is even harder to find any studies conducted on hackers, as noted by Rogers on his website, "While working on my doctorate I became frustrated with the lack of any central reference sites that dealt with psychology and cyber related deviance" (Rogers, 2003b).

> Many researchers and journalists have provided descriptive accounts of hacker's motivations and developed profiles from interviews and surveys of those that have been apprehended. However, behavioural scientists have provided little or no empirical research in the areas of psychological profiles and causes of hacking behaviour (Karnow et.al, 1994) (Karnow et.al, 1994 as cited in Beveren, 2001).

This lack of research is due in part to society considering what civilian hackers do as illegal, which causes difficulties recruiting volunteers for studies. "The global and anonymous nature of computer-mediated communication exacerbates such problems because any attempt to generate a research population from the computer underground will necessarily be self-selecting and it will be difficult to check the credentials of each subject" (Jordan & Taylor, 1998). Rosteck also states his confusion of why no sociological research has been done on the hacking community when they are part of the widely accepted *Information Society* (Rosteck, 1994). The available resources are based on very informal and usually not face-to-face interviews or stories as told by hackers. Hackers prefer to remain anonymous, only known to others by their screen names. Even if a study was initiated, their desire and requirement for anonymity would present an obstacle.

A major limitation is the lack of defined jobs, tasks, and skills for cyberspace warriors. Normally, a task analysis is completed to determine what skills, abilities, and knowledge are necessary for new recruits into a specific job. . "…selection procedures must be based on a job analysis" (Gatewood & Feild, 2001). Without knowing what the job is, it is difficult to complete the recommended job analysis. Without the analysis, a test is difficult to create. This limitation is also at the heart of this research. Without the known tasks, the Air Force must create the tasks, select candidates for employment and training and then update and improve the criteria as more is learned.

The limitations regarding test development are the most prohibitive and in some sense, an accumulation of some of the other limitations. To properly develop a test, a cadre of experts is required. The experts should include content experts, test-writing experts and possibly experts in the cyberspace organization. As previously indicated the cyber force skills are in an identification phase and the Air Force does not yet know who the cyberspace experts are. The Air Force has resources for test writing but with so little known regarding the content, even they will face challenges. Experts in the organizations' culture would be useful to ensure the selectees will *fit-in* to the organization. Such experts will not be available until these organizations have not only formed, but also developed their own culture. The test will require content experts in the areas that are deemed necessary. These areas may include networking, programming, vulnerabilities, and applications just to name a few. Even once all the expertise are identified, the test writing process requires a great deal of time. The test writing process and its associated limitations are further addressed in Chapter III and Chapter IV.

The methodology also presents limitations. Although every methodology has its distinct set of limitations, the different methodologies used each provide unique and valuable information regardless of their limitations. A limitation associated with methodology is that the most scientific and preferred methodology is not always consist with they type of research being conducted. Therefore, the methodologies are limited by the information and resources available, the type of research being conducted, and the scope of the research. The benefits and limitations of the specific methods used are addressed in Chapter III.

1.5 Scope

The Joint Chiefs of Staff definition for cyberspace includes many different aspects. Considering how to select candidates for all cyberspace aspects are beyond the scope of one thesis. Some of the aspects may require unique filtering procedures based on specific skills, knowledge and abilities needed to perform that task. Although all aspects of cyberspace are important, this research is focused on the network portion of cyber operations. Network operations refer to what is known in the military as network attack and network defense. Network cyber operations do not include the day-to-day maintenance and operations of the infrastructure, systems, and applications that are the military network. Cyber operations are an instrument of war fighting. In the pursuit of cyberspace warriors, the filtering process should separate those that can maintain the network from those that can fly and fight in cyberspace. Hopefully, many aspects of this research will be beneficial and possibly replicable for some or all of the other aspects of cyber operations.

This research is written at the operational level. The strategic level of aptitude testing and career development would include all aspects of cyberspace, not just the network portion, and the relationship of cyber missions to other missions. An approach at the tactical level should include an actual test proposal with instructions for use. As previously stated, that is not yet possible but is recommended as the logical progression of this research. Therefore, this research provides the foundation for developing tests and filtering methods and implementing them at the tactical level. The results will suggest a

direction the Air Force can follow for designing tests, implementing tests and selecting cyberspace warriors through a rigorous selection process.

The content analysis portion did not consider motivations and skills associated with the insider threat. "[A]n insider has much more access than someone outside the organization" (Schneier, 2000). Because they already have this type of knowledge and access, they are not what are considered a hacker for the purposes of this paper. External hackers are the subject of the research because cyberspace warriors will not have insider knowledge. They will have to approach the problem with the same resources as an external attacker does.

This research only addresses selection processes for Air Force personnel. All components of the Air Force, active, reserve and National Guard can follow the selection process discussed and proposed here. However, selection processes for the other services, such as the Navy, Marines, or Army are not considered. This limitation is for two reasons. First, cyberspace operations are an Air Force mission. Although the other services may be performing similar operations, the Air Force is the only one that has officially stated its intent to perform the cyberspace mission. The other reason is because the selection processes addressed are Air Force processes. Many of the recommendations made here will be directly transferable to the other services, however, the research and recommendations were based on current Air Force selection methods. Even if the research and recommendations are not directly transferable to the other services, the information provided here should be useful if any decide to undertake a similar mission.

1.6 Assumptions

In order to complete a thesis regarding the selection method for cyberspace warriors, some assumptions are necessary. The first is that the military is dedicated to the cyberspace mission and is willing to dedicate resources to fulfilling the mission. These resources include time, money, and personnel in an effort to establish the criteria for becoming a cyberspace warrior and to implement the necessary filtering processes. This could imply significant changes in existing testing methods. Another assumption is that there will be a cyberspace career field or multiple career fields. There is the possibility that a new career field will not be created. However, this is unlikely, as this mission will require some special skills and significant training and experiences will be necessary. Therefore, a new Air Force Specialty Code (AFSC) is an assumption used within this thesis. The assumption that both enlisted and officer AFSCs will be created is another assumption. Although some AFSCs, such as pilots and navigators are only available to officers, at this time, it is assumed that cyberspace is a mission that enlisted and officers will perform. Among other considerations, this could change depending on what skills and education is determined to be necessary. Another assumption is that only Air Force personnel are considered for cyberspace operations. As addressed in the *limitations* portion of this chapter, cyberspace operations are an Air Force mission and the research and recommendations provided here are intended for the Air Force to use. Furthermore, although it is highly likely that civilians or contractors will be part of the cyberspace mission, their role is more unpredictable than the military's at this point.

1.7 Thesis Layout

This chapter provided the background necessary to identify the problem and propose a possible solution. This chapter also provided the framework for the problem and solution by identifying the scope, limitations, assumptions, and definitions necessary for the remainder of the thesis. The following chapters address the problem and proposition in an organized manner that ultimately culminates in suggestions for and a methodology to develop a test for potential cyberspace warriors. This progression begins with a literature review. The literature reviewed serves three main purposes: to explain why a cyberspace force is necessary, to demonstrate the acceptance and use of tests for important jobs, and to identify the qualities desired in this new force based on findings from the hacker community. Chapter II closes with a synthesis of those seemingly separate ideas into an argument for the development of tests and other selection processes for potential cyberspace warriors. Chapter III continues by explaining the methodologies used for this research. The research used a combination of a literature review and a content analysis that allowed for the application of garnered knowledge to scrutinize an existing test and propose a methodology to develop a new test or improve existing tests. Chapter IV will provide the results of the research, which include the content analysis results and their use to scrutinize the existing test. Additionally, recommendations for improving tests and/or developing new ones and recommendations regarding other selection options are provided. Chapter V concludes by final offering thoughts on the many aspects of this thesis and recommending topics for future research.

II. Literature Review

2.1 Introduction

This chapter summarizes the literature reviewed to understand the research problem and support the proposed proposition. First, it is important to understand why the Air Force is assuming the cyberspace mission. This understanding includes a brief history of events that lead to the assumption of a cyber mission by the Air Force and a brief discussion of actions to implement the mission. Next is a review of successful aptitude tests. The intent of this section is to prove that testing is a reliable and useful way to screen applicants. The third section is a review of the articles and books relating to computer hackers' skills and motivations. "Unfortunately, not much is known about true adversaries, but gross characteristics and behaviors can be adopted and examined based on analogy to types of other real-world adversaries and on analysis of current, real-world threats and attacks" (Lowry, 2001). This section provides the preponderance of data used for the content analysis. Together, the three sections establish the need for a military cyberspace mission and the background for how the military can approach a solution to this need through the use of valid and reliable tests based on the skills and motivations of those who are already exploiting cyberspace.

2.2 Cyber Mission

2.2.1 Identifying a Need.

In 2003, cyberspace was referred to as "the control system of our country" (Bush, 2003). This reference is to the military, public, private, academic and government settings. Our nation's dependence on cyberspace makes it our Achilles' heel. "…its overwhelming military superiority and its leading edge in information technology have also made the United States the country most vulnerable to cyber-attack" (Adams, 2001). As the nation becomes more dependent on technology and cyberspace, it becomes more important to protect and defend it and ensure its security and availability.

Concerns regarding our reliance on information systems have existed for decades. One of the first noteworthy actions was President Jimmy Carter's 1979 Presidential Directive 53, which identified communications to be a necessary component of the National Security Emergency Preparedness. (Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, 1989) Continuing concern for cyberspace security has grown as cyberspace and our dependence on it grows. The *National Strategy to Secure Cyberspace* was released in 2003. This document acknowledged the importance of cyberspace to our nation and indicated that everyone is responsible for the protection of cyberspace,

> The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society-the federal government, state and local governments, the private sector, and the American people. (Bush, 2003)

Although the importance of cyberspace to our nation is accepted, "… the healthy functioning of cyberspace is essential to our economy and our national security" (Bush,

2003). The military was not tasked with protecting cyberspace, "In general, the private sector is best equipped and structured to respond to an evolving cyber threat" (Bush, 2003).

Even without direction, the military recognized the need to exploit cyberspace. "Our ability to fight in Ground, Sea, Air, and Space depends on communications that could be attacked thru Cyberspace" (Wynne, 2006). Hackers and insiders are a major concern to the protection of information on networks and to the networks themselves. The military has implemented a defense in depth posture to protect the network and its resources. Everyday the military monitors intrusion detection systems and collects data to monitor for intruders or manipulation of data. Defense is not enough. The military must prepare to use cyberspace as an active military war-fighting domain.

> When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies. (Bush, 2003)

2.2.2 Development of a Command.

The military, and the Air Force in particular, recognizes the potential of cyberspace operations. "…Cyberspace is a Domain on which many rely and in which war fighting can, and, actually by some definitions already, takes place. One rough and ready demonstration that Cyberspace is a true Domain on a par with Land, Air, Space and Sea is to apply the basic questions of the Principles of War" (Wynne, 2006). The Air Force has identified cyberspace as a war-fighting domain and is taking the lead to prepare. In a Letter to Airman, Secretary of the Air Force (SECAF) Michael Wynne and Chief of Staff of the Air Force (CSAF), Gen T. Michael Moseley, announced the U.S.

Air Force had adopted its mission to include cyberspace (Wynne & Moseley, 2005). According to Libicki, this was probably the right step. "Conflict in cyberspace, like conflict in predecessor media, must be dealt with in its own terms and may justify entirely new missions and organizations" (Libicki & Shapiro, 1999).

Once Cyberspace is recognized as a place to fight a war and therefore a part of national defense it is necessary that the "…primary responsibility for the cyber-defense of the nation must be given to the Department of Defense" (Adams, 2001). As part of the Department of Defense, the Air Force is the youngest of the services and recognizes that when a new war fighting domain is identified, it requires new doctrine, new culture, new people, and a new home (Libicki & Shapiro, 1999). SECAF Wynne stated that the new mission is a way to "…recognize the existing fact that significant Air Force personnel and technology have long been engaged in fighting in Cyberspace" (Wynne, 2006). Furthermore, the current Air Force Strategic Plan identifies cyberspace as a core competency and calls for

> …processes and requirements that define the Air Force's contribution to offensive and defensive operations in cyberspace. These will present increased and more flexible options for COCOMs and warfighters to compress the digital kill chain, enable information warfare, and advance beyond all competitors in the medium." (AF/A8, 2006)

There are concerns about the Air Force taking on the primary role of the cyberspace mission. Each service and government organization already uses technology and has developed ways to use cyberspace as either a support function or a mission or both. "Every service has developed its own information-warfare capability at huge cost and with significant duplication of effort. Similarly, the CIA, the Defense Intelligence Agency, and the NSA have each undertaken independent information-warfare efforts,

with little cooperation between them" (Adams, 2001). Additionally, just because the Air Force recognizes the need and is creating a new mission does not mean they are necessarily the best to control cyberspace. "But history also suggests that institutions that have mastered one new medium are not automatically assigned the next. After all, the U.S. space program grew out of work undertaken by the *Army* at Redstone Arsenal" (Libicki & Shapiro, 1999).

> The Air Force recognizes its responsibility to others in the Cyberspace realm. This is a Battle Domain in which the Air Force operates with, and supports our sister Services, first responders, and many times Non-Government Organization and the many non-military authorities who also work to keep Cyberspace secure. There are many partners across this Domain. (Wynne, 2006)

The cyberspace mission is not only fought by the Air Force. "This Duty is joint, and, as I have noted, it is Interdependent. The duty is to bring to the Fight what the Air Force has to offer, and to exercise good stewardship of the Air Force personnel and resources that are in some cases already devoted to operations in Cyberspace" (Wynne, 2006). SECAF Wynne also acknowledged that as a war fighting domain, Cyberspace is controlled by the Combatant Commanders and SECAF Wynne therefore consulted with Gen James Cartwright, U.S. Strategic Commander, to ensure the Air Force provides Combatant Commanders with "…organized, trained and equipped Cyberspace Forces" (Wynne, 2006).

Now that Cyberspace is recognized as a Department of Defense responsibility, and furthermore, the Air Force has assumed responsibility for it, the Air Force must determine how to integrate this mission into the Air Force structure. To do this, CSAF Gen Moseley and SECAF Wynne plan a Cyberspace command that is "…a peer with Air Combat Command and Air Force Space Command" (Wynne, 2006).

2.2.3 AF Career Development.

Along with the assumption of the new mission comes the responsibility of organizing, training, and equipping cyberspace forces. SECAF Wynne recognizes this and said that "Air Force military and civilian experts are working now forming the career and school paths that will ensure a full career with full opportunities for advancement to the highest ranks of the Air Force" (Wynne & Moseley, 2005). He and CSAF Gen Moseley "tasked the Commander of Air Education and Training Command to develop a training plan…" (Wynne, 2006). "Good stewardship means attending to the systematic training, organizing, and equipping that is our job. This includes especially attending to the career progression of the Airmen involved in Cyberspace, including our guard, reserve, and civilian professionals" (Wynne, 2006).

2.3 Aptitude Tests

2.3.1 General.

"Almost concurrent with commercial development of the computer was psychological research and a proliferation of psychological instruments which attempt to identify the aptitudes which lead to success in selecting and training the human side of computation" (Mayer & Stalnaker, 1968). The U.S. military in particular is fond of the aptitude test. "Cognitive testing is prevalent in the military, playing an important role in selection and placement" (Miller, 1999).

> Time and again, in research and operational settings alike, aptitude has been shown to matter. Not only do higher ability military personnel do better in job training, but level of aptitude has distinguished fighters from non-fighters during

> the Korean Conflict[8], been found to be relevant in specific jobs such as armor crewmember, general vehicle repairman, supply specialist, and cook[9]. (Laurance, 2004)

Potential enlisted and officers take aptitude tests to place them in fields they are likely to succeed in and to prevent them from placement in fields where they are not qualified or skilled.

There are critics of aptitude tests and certainly some limitations to them. "Aptitude tests are sometimes criticized for seeking to predict success in training programs rather than to predict success on the job" (Ebel, 1972). Test developers are aware of this limitation and studies, as noted in some of the specific reviews, attempt to account for this by altering the definition of success and completing long-term studies to ensure the test predicts in the long-run what it attempts to predict with short-term indicators. Another limitation is the definition of success in an aptitude test and measuring success, however it is defined. "Predictions of success are useful only to the degree that success can be reasonably defined" (Ebel, 1972). For example, some consider success in college the attainment and sustainment of a minimum grade point average while another person may disregard his/her grades but judge success by the end goal of college graduation. "To the Military, success in training is, and will continue to be, the most important criterion for prediction" (Welsh, John R. Jr., Kucinkas, & Curran, 1990). Even if one is successful in training for a skill that does not necessarily mean that person will be successful in the working world. There is definitely a difference in culture and pressure of the classroom when compared to the real world. However, "…criteria of success in training programs are easier to define and to measure than criteria of on-the-job success" (Ebel, 1972). Although much more than aptitude is necessary to be

successful in the work place, it is important to remember that training is to prepare the student to be successful in the work place; therefore, "If there is evidence of unreasonable disparity between competence in training and competence on the job, it may be the training program rather than the test that is in need of correction" (Ebel, 1972).

Since we have recognized that aptitude and skill are not the only important aspects for success in the real world, it is important to consider what other factors contribute to success in the real world and decide if they can also be measured in some way to assist individuals in choosing careers. "[I]n a study of IS professionals, found support for the hypothesis that individuals are attracted to positions in which their personality and talents are matched with the demands of their position and perform significantly better when this is achieved (Ketler and Smith 1993)" (Ketler and Smith 1993 as cited in Kakabadse, Kouzmin, & Chatham, 2002). If this is true, it is important and relevant to consider personalities of potential cyberspace warriors. "The Myers-Briggs-Type Indicator (Meyers and Briggs 1975) has achieved the most credibility in the literature and empirical research" (Kakabadse et al., 2002).

2.3.2 Review of Specific Tests.

The literature review of aptitude tests focuses on tests that are widely known and generally highly regarded. It is the purpose of this section to demonstrate that aptitude tests, when developed and administered correctly, can and do assist in selecting individuals into situations where they are likely to be successful. If the literature can show that aptitude testing is useful then it will be validated as a way to select individuals for a career in cyberspace as dictated by their aptitude.

2.3.2.1 ASVAB

In order to help determine eligibility and assist in training selection for potential enlisted recruits, the military has adopted one test. "The Department of Defense uses a single battery, the Armed Services Vocational Aptitude Battery (ASVAB) to determine the enlistment eligibility of applicants for the Army, Navy, Marine Corps, and Air Force, as well as their respective Reserve Components" (Sellman, 2004). "The Armed Services Vocational Aptitude Battery (ASVAB) has been in use in the United States since the late-sixties and has been updated regularly since its implementation. It is used to evaluate basic enlistment eligibility and to determine vocational placement" (Miller, 1999). "It was scientifically developed and validated to ensure that all enlistees would have a reasonable probability of completing military job skill training and performing successfully on the job" (Sellman, 2004). The ASVAB is a norm-referenced test because it scores candidates based on the youth population instead of attempting to predict a person's specific level of performance in a specific area (Laurance, 2004). "Because of extensive use of the ASVAB for selection and classification into all services, numerous studies of its predictive validity have been undertaken" (Miller, 1999). "The construct and content validity of the ASVAB were established through a number of well-known multiple-aptitude batteries" (Welsh, John R. Jr. et al., 1990). Studies have found the ASVAB is reliable and useful, "The Services need to select and classify appropriately the most trainable applicants. The ASVAB composites have a clearly demonstrated validity for that purpose" (Welsh, John R. Jr. et al., 1990). The ASVAB helps the military because "Screening on the basis of aptitude and education credentials advances the

organizational goals of maximizing technical performance and minimizing attrition" (Laurance, 2004).

Besides internal consistency and reliability, it is important for this test to predict how well military members will do in their respective jobs. In a comprehensive review of literature and data, Welsh et. al found "The primary conclusion from the review of the literature is that the ASVAB aptitude composites and Armed Forces Qualification Test (AFQT) are valid predictors of final school grades, self-paced technical school completion times, first-term attrition, and job performance measures" (Welsh, John R. Jr. et al., 1990). Sellman's 2004 report cites six studies that show "…a strong relation between ASVAB (including AFQT) scores and success in military job skill training and hands-on job performance across a range of occupations" (Sellman, 2004). Laurence makes the same claim that "Decades of study results have affirmed that recruits who scored higher on the ASVAB also perform better in training and on the job" (Laurance, 2004).

The ASVAB continues to improve. Recently, a computerized version of the ASVAB has been put into use. In addition to this change, efforts have been made to increase the predictive validity of the test. This Enhanced Computer-Administered Test (ECAT) is composed of tests that supplement existing measures, not duplicate them.

> [T]he ECAT tests have been shown to be effective in increasing the predictive ability of the ASVAB. Wolfe (1997a) reported that although the ECAT battery adds significantly to the prediction of training criteria based on both the final school grades and hands-on performance, the increase in predictive validity is greatest for hand-on performance. Averaged over several Army, Navy and Air Force schools, the ECAT tests enhanced prediction of the final school grades by 1.9% whereas they increased prediction of hands-on performance tests by 6.6%. (Miller, 1999)

Obviously, the test is getting better and better at predicting success.

The ASVAB is not only used for military enlistment eligibility and job classification, it is also administered to high school and post-secondary students as part of a Career Exploration Program (CEP). The CEP is a combination of the ASVAB and an interest inventory. This combination is used to assist students in determining which careers they are suited for and in which they have an interest in both the military and civilian communities. Sellman cites previous work that shows the CEP is valid for use as a predictor of job performance in various civilian occupations and a study that links ASVAB scores to the Department of Labor's General Aptitude Test Battery that also has high validity for the civilian work force. (Sellman, 2004)

2.3.2.2 Pilot Selection

Although potential enlistees for all services are classified using the same instrument, potential officers are evaluated differently. Except for Academy recruits, the primary selection tool for potential Air Force officers and their career field is the Air Force Officer Qualifying Test (AFOQT). Some career fields require other screening methods to ensure the candidate is capable of success in the career. One such example is the pilot selection method in the U.S. Air Force. The U.S. Air Force pilot candidate selection method (PCSM) consists of the following considerations:

1. Physical qualification
2. Eight tests from the AFOQT which form the pilot composite
3. The Basic Attributes Test (BAT)
4. Flying experience

However, “The indicators of pilot aptitude that are used vary by source of commission” (Carretta, 2000). For example, the Air Force Academy (AFA) has no minimum AFOQT score for candidates and does not consider race, gender, or ethnicity in selection. The AFA considers factors such as academic, military, and athletic performance. Each candidate submits a package with the required information and the packages are reviewed by a committee. Officer Training School (OTS) candidates also submit a package for review. The package includes such things as AFOQT scores, employment history, letters of recommendation, and flying certifications. These packages do include race, gender, and ethnic data and the committee determines selection based on the *whole person* concept. Reserve Officer Training Corps (ROTC) candidates are rank ordered according to items such as their Relative Standing Score (RSS) that are based on detachment commander’s evaluations, AFOQT composite scores, GPA, etc. Carretta found that although pilot aptitude tests are required for all pilot candidates, different selection boards use the scores in varying degrees to select candidates (Carretta, 2000).

The pilot selection example demonstrates how to use test scores in conjunction with other factors. Based on the scores associated with the different criteria, candidates receive PCSM composite score. Caretta’s research revealed that higher PCSM composite scores predict the following:

1. Greater probability of completing training
2. Fewer hours to complete training
3. Higher class rank
4. Greater likelihood of being fighter qualified

(Carretta, 2000)

Carretta compared the differences of commissioning sources when selecting pilot candidates. He found that

> The two largest sources of USAF pilots (AFA and ROTC) place a much greater emphasis on measures of officership (AFA – military performance average, ROTC – RSS) than measures of ability (e.g., academic performance, flight screening performance, aptitude test scores) when selecting pilot trainees. This is rather perplexing in the absence of studies showing validity for measures of officership for predicting pilot training performance. (Carretta, 2000)

Ultimately, Carretta concluded that along with the PCSM score and selection boards, pilot selection criteria should include interviews and personality measures.

2.3.2.3 SAT

Another test that deserves consideration is the most widely used test - the SAT Reasoning Test (Kobrin & Michel, 2006). The SAT is a valuable aptitude test to reference because of its long history, popularity, and use outside of the military. The SAT, in some form, has been in existence since 1926 and 1.3 million examinees take the test every year (Young & Kobrin, 2001). Another reason to review it is because it has been significantly researched and proven, "Over the years, hundreds of validity studies have been conducted with SAT verbal and math scores (SAT V+M) and high school grades (HSGPA) as predictors and with freshman grades as the criterion" (Camara & Echternacht, 2000). "The SAT has proven to be an important predictor of success in college. Its validity as a predictor of success has been demonstrated through hundreds of validity studies" (Camara & Echternacht, 2000).

The SAT is intended to predict a person's success in college. One problem for the SAT, and other tests as previously noted, is defining success. In Burton and Ramist's long-term study of SAT scores and college success, they defined success in terms of

cumulative grade average and graduation. They used the first-year grade average as a measure of success and found it was reliable in predicting the overall grade average (Burton & Ramist, 2001). The Burton and Ramist study is similar in style and outcome to Wilson's 1983 long-term study. "Both reviews found that SAT scores consistently made a significant contribution to predicting success in college as defined by college grades; both found that the combination of SAT scores and high school records provided better predictions than either predictor alone" (Burton & Ramist, 2001). Furthermore, the Burton and Ramist study also found "…that the SAT and high school record are significant predictors of graduation" (Burton & Ramist, 2001). Therefore, when success is defined as grade average or as graduation, the SAT is a proven predictor of success, especially when combined with high school records. "SAT scores and high school records have established their place in the college selection process" (Burton & Ramist, 2001).

These studies point to many considerations when choosing a test to administer or when selecting artifacts to use to determine success. When choosing a test, one must ensure the test is a measurement of what is intended to be measured. When a proxy for a desired outcome is used, which is common, it must be clear that that proxy is truly related to the desired trait. Camara and Echternacht determined that freshman grades are more reliable than cumulative grades when evaluating admissions because freshmen take similar classes so it is easier to correlate the data. They also found support that freshman GPA is a good predictor of overall GPA. Furthermore, they found evidence to suggest that admission predictors are highly related to graduation. Therefore, freshman GPA is a good predictor of graduation (Camara & Echternacht, 2000). Selection of artifacts refers

to considering more than one test or item as the sole source of admissions or success predictors. As previously noted, multiple studies have demonstrated that success in college is best predicted when high school grades are considered in addition to SAT scores (Burton & Ramist, 2001; Camara & Echternacht, 2000; Ramist, 1984). "The combination of the SAT score and high school record has the highest correlation observed. This result is also found commonly in the literature" (Burton & Ramist, 2001). These results indicate that one test is not a suitable determinant for success. Although a single test is useful, its value increases with additional measures.

2.4 Hacker Traits

The word Hacker has different meanings to different people. Part of the problem is that they can be classified in different ways depending on the research intent, point of view, and desired use. Psychologists may need to classify them according to motivation, law enforcement may classify them according to damage inflicted, or security experts may classify them by skill level. Rogers noted the problem for researchers attempting to study hackers and tried to consolidate many theories by categorizing hackers in his work *A New Hacker Taxonomy*. His proposed taxonomy divides hackers into seven categories according to their technical abilities (Rogers, 2003a). Rogers noted previous methods for categorizing hackers such as "…a classification system based on the activities the hacker was involved in" or "…hacker's activities, their prowess at hacking, their knowledge, motivation, and how long they had been hacking" (Rogers, 2003a). Even the hacking community has its own "loose hierarchy" (Rogers, 2003a). Rathmell classifies attackers

into three categories, "…hackers, criminals and politically motivated sub-state groups" (Rathmell, 1997). He further divides the hacker category into amateurs and professionals differentiating the two based on their background and motivation. (Rathmell, 1997)

In order to determine what traits a cyber aptitude test should consider, a search for studies on hackers was attempted. Due to the underground nature of hacking and the relatively few who have been caught, scientific studies of actual hackers to include their training – formal or informal, their beliefs, their thought processes, characteristics, traits or anything else was unavailable. Therefore, in order to determine what a cyber aptitude test should cover, a content analysis of literature that describes hackers was completed. Through this content analysis, identification of the common motivations and skills of computer hackers was realized.

Although many different types of hackers exist, with different motives, skills and outcomes,

> Hackers say they are particularly concerned that computer security professionals and system managers do not appear to understand hackers or be interested in their concerns. Hackers say that system managers treat them like enemies and criminals, rather than as potential helpers in their task of making their systems secure. (Denning, 1990)

The military has been concerned with any entity that attempts to penetrate the network or its resources without the proper authority. Schneier verbalizes the concerns.

> I don't buy the defense that a hacker just broke in a system to look around, and didn't do any damage. Some systems are fragile, and simply looking around can inadvertently cause damage. And once an unauthorized person has been inside a system, you can't trust its integrity. You don't know that the intruder didn't touch anything. (Schneier, 2000)

In the past, the importance of learning and knowing about hackers has been to prevent them from gaining access to systems and programs and when they do get in, being able to

find and remove them, and patch the holes they breached and any they created, and restore any data or systems that were damaged. Nissenbaum provides a definition of the hack that sums up what the military is concerned with, "To hack was to find a way, any way that worked, to make something happen, solve the problem, invent the next thrill" (Nissenbaum, 2004). In general, these attackers have some general characteristics; however, the attackers' motivation and skill level may be useful in predicting what type of data and systems the attacker might target, what he may do with the data once access is gained, and what exploits and tactics he may use.

For our purposes and the sake of simplicity, we will differentiate between three types of attackers: hackers, crackers, and cyber terrorists. The purpose here includes identifying motives, skill level, and threat level. Hackers like to consider themselves social activists, fighting for the first and fourth amendments, encouraging system administrators, and programmers to better protect their networks and software, respectively. "… one hacker says that the ease of breaking into a system reveals a lack of caring on the part of the system manager to protect user and company assets, or failure on the part of vendors to warn managers about the vulnerabilities of their systems" (Denning, 1990). "Hackers say that system managers treat them like enemies and criminals, rather than as potential helpers in their task of making their systems secure" (Denning, 1990). Hackers do break into systems but not for gain beyond demonstrating their skills to be able to break in. They rarely steal, copy or destroy data, unless that makes their point, as in a web site hack. Their intent is to prove to others within and external to their community that they can beat the security that is in place. This type of hacker is actually offended by those they refer to as crackers. Crackers are those who

break into systems, not for the enjoyment and challenge it provides, but to steal, copy or damage data to incur financial gain for themselves. "Hackers say they are outraged when other hackers cause damage or use resources that would be missed, even if the results are unintentional and due to incompetence" (Denning, 1990).

One perplexing contradiction of hackers is a similarity they have with researchers and scientists.

> "… [I]n the same way scientific researchers allow all others in their fields to be tested and developed further, hackers who take part in the Linux project permit all others to use, test, and develop their programs. In research, this is known as the scientific ethic. In the field of computer programming it is called the open-source model." (Himanen, 2001)

There is even a third type of hacker, the cyber terrorist. The FBI defines cyber-terrorism as "…the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (Rogers, 2000). Puran differentiates cyber-terrorists from other cyber attacks and hackers with the following:

> Attacks have specific objectives and/or victims such as opposing religious groups information systems, cyber-terrorist purpose is to create fear of the group and advance their own agenda or gain fellowship, destroy the enemy's capabilities to operate, persuade others to believe the victim is vulnerable and negligent and to increase loyalty and pride within their group. (Puran, 2003)

Rogers defines a cyber-terrorist as "An individual that uses computer/network technology (i.e., networks, computers, Internet) to cause intense fear; one who uses computer/network technology to control, dominate, or coerce through the use of terror in furtherance of political or social objectives" (Rogers, 2000).

A category that is intentionally ignored is the insider. This is a predominant threat and should not be ignored in either the military or the civilian community.

According to the 2005 CSI/FBI report, inside attacks are approximately equal to external attacks (Gordon, Loeb, Lucyshyn, & Richardson, 2005). However, they pose a unique threat to information system security professionals. The insider has different motivations for his/her attacks. He/She also has an advantage of already having access to information and accounts that outside attackers probably do not easily have. This research is not intended to address the unique challenges of the inside attacker.

This research is predominantly focused on defining hacker skills and motivations. They are the subject of this research because the Air Force is still struggling with defining what a cyberspace warrior is and needs to search outside of itself to identify this new warrior. Although civilian computer hackers perform what many consider immoral or illegal activities, there is no argument that they have the skills that military cyberspace warriors will need and they have an intrinsic motivation that the military may be able to leverage to select individuals that are likely to be successful in the military mission of cyberspace. If these skills and motivations can be identified then the military can work to look for the same skills and motivations in people with the right morality and the qualities the Air Force requires.

2.5 Synthesis

Although the three topics presented here may appear unrelated and possibly arbitrary, they are all necessary in relation to the problem statement. The cyber mission portion explains the reasoning behind the development of a cyberspace mission for the Air Force. It is important to know why a new mission is initiated and what that mission

will add to existing military capabilities. The military, government, academia, and civilian sectors have recognized our country's dependence on cyberspace and therefore our vulnerability to attack. As the protectors of the nation, it is only natural that the military prepare and plan to defend this resource. Furthermore, it is now viewed as not just a resource of the United States that must be defended, but as a resource to use against adversaries. Other nation states or organizations that depend on cyberspace are also vulnerable to attack and this knowledge must be used to fight against our adversaries. To truly leverage cyberspace for our purposes, it is important to recruit the right people. Recruiting the right people is difficult. Nelson and Todd acknowledge that "While no single approach is guaranteed to ensure that you always hire the right people and do so in the most cost-effective fashion, there are some things you can do to improve the odds of finding the right people, making good hiring decisions and closing the deal" (Nelson & Todd, 2004).

Tests will help improve the odds of selecting the best candidates if the tests are proven to be effective. Testing is not only an acceptable way to screen candidates, but that testing has a long and viable history that has worked well in the military and academic settings. The test literature also shows that the military is well equipped to develop tests that can filter potential cyberspace warriors from the general populous by way of the ASVAB for enlisted personnel or screen officer candidates in a similar fashion as pilot selection. Some of the criteria to use in these tests will come from the identification of traits, knowledge, and skills that one must poses to be a successful cyberspace warrior. As we do not have such existing standards, the identification of hacker traits is a starting point for identifying what type of skills to include on a test for

cyberspace warriors. The literature regarding hackers' skills, motivations, characteristics, knowledge, and abilities is used as a way to identify the skills and motivations the Air Force will need in cyberspace warriors. No matter what characteristics, traits, aptitudes, and/or skills are determined to be necessary for cyberspace warriors, it is important to remember that people in this field will not work alone. They will be part of a team and must also have the skills, personality, and characteristics to work in that environment. Kakabadse et al. explain that skill and talent alone are not enough to ensure success in environments where success is dependent on team performance. "Skill and talent have to be supplemented by a set of qualities of character and temperament which enable the individual to harness and focus on other talents, and make them effective" (Kakabadse et al., 2002). The identification of hackers' skills and motivations will be used to propose screening tests and techniques so the Air Force will have cyber warriors that have the best chance of being successful.

Determining what method to use to asses potential candidates is difficult. Gatewood and Field suggest the following questions guide selection measures:

> 1. Have job applicants previously demonstrated past behaviors associated with successful performance of the tasks of the job? If so, evaluation of past performance, such as through a biographical data questionnaire, may be appropriate.
> 2. Can job applicants be observed performing the job or part of it? Is there a means for simulating the job in a test situation that is likely to require important behaviors as defined by the job? If so, is there a practical way of measuring performance? When demonstration of successful performance is possible and measurable, a work sample or performance test might seriously be considered.
> 3. Would a written test be best for examining worker requirements in terms of eliciting desired reactions and providing practical scoring? If so, a written test should be proposed. A paper-and-pencil test is often appropriate to assess job knowledge.
> 4. Would an opportunity for job applicants to express themselves orally through an interview cover job requirement that might go unassessed using other means?

In this case, a structured selection interview that can be objectively scored could be administered.
5. Can the assessment method produce reliable and valid data for evaluating job applicants' possession of a KSA? If not, the method should be dropped form consideration.
6. Is it practical and within our resources to use a particular method for measuring a KSA? If not, an alternative method should be considered. (Gatewood & Feild, 2001)

2.6 Summary

This chapter provided a summary of the major literature areas that are needed to address some of the challenges the Air Force is facing in determining who the cyberspace warriors are. The first section laid a background for understanding why the Air Force is assuming the cyberspace mission. Cyberspace is important to our country and our way of life, and not only do we need to protect it for that reason, but we also need to treat it as a domain in which we fight. Now that the Air Force has accepted the mission, it must determine how to select people to work in this mission area. One way that has long served academia, and especially the military, is through the use of reliable and valid tests. Based on the history of testing processes and success, this seems to be the natural way to select individuals for this mission. However, since the mission is new, it is difficult to identify what content the test should contain. The method recommended here is to determine the skills and motivations of hackers and use those to develop a test for potential cyberspace warriors.

III. Methodology

3.1 Introduction

This chapter focuses on the way the research was conducted. This chapter will introduce and explain the different methods used throughout the research. These methods include a literature review, a content analysis, a test critique, and a review of how to develop or improve a test. Because this research was the consolidation of different fields, a synthesis of how these methodologies were combined is presented.

This thesis is based on two principal methodologies. The first is a literature review. Although a literature review is a critical chapter for all theses, it is especially important when little to no research has been published on the desired topic. In the latter case, it is very important to read the literature in closely related, well-researched, and published areas and then combine relevant knowledge of these disciplines and use it as a basis for the new discipline. Therefore, the literature review in this thesis is the foundation for this thesis. It was intended to show that an aptitude test is a possibility the Air Force can use to filter those recruits with a potential for success in this field. It is also used to determine what skills should be tested, and how to develop a test for this type of force. Gatewood and Field address the problems of personnel selection for new fields. They recommend "Individuals within the organization who can envision what the job will be like should be selected. In addition, others who may be outside of the organization but have specific technical knowledge about the needed changes should be considered"

(Gatewood & Feild, 2001). The second methodology is a content analysis of the hacker related materials.

3.2 Overall Theory

The foundation of this research is that computer hackers contain the skills, knowledge, abilities, characteristics, and motivations required for potential cyberspace warriors. In order to determine the necessary aptitudes and motivations for cyberspace warriors, the military should identify the aptitudes and motivations of computer hackers. Based on hacker skills and motivations, the military can determine which skills and motivations reflect those they desire in cyberspace warriors and then the military can target people with those aptitudes and motivations.

Although specific computer knowledge and skills are necessary, they are only part of the equation of a valuable cyberspace warrior. "The underpinnings of job performance include knowledge, skill, and motivation" (Laurance, 2004). Knowledge and skills can be taught, motivation is less malleable "We know that high motivations often overcomes low aptitude, while low motivation can defeat high aptitude" (Lowe, 1998). Therefore, motivation is an important consideration in selecting candidates. This quote also raises the concern of where does aptitude overtake motivation and vice versa. Although skills and motivations are not the only predictors of success, these are the core factors in the selection process. Other factors that may predict success include learning styles and/or teaching methods. If the student's learning style and the teacher's methods are not conducive, the student will have to work harder to be successful which indicates the

student will need a higher motivation factor for success. However, the intent of this research is to determine a way to select candidates with the highest probability of success; therefore, factors that are not of importance in an initial screening process or cannot be measured in the process are left for others.

The upper-left box on the Table 1 indicates the people that should be highly recruited for work as cyberspace warriors. The lower-right box indicates those that should not be considered. The other two boxes are of concern. Aptitude and motivation are not Boolean, they exist on a continuum, meaning that low motivation, or low aptitude does not necessarily indicate complete lack of motivation or aptitude, respectively. One of the problems resides in determining where on each scale an individual lies. Another difficulty is deciding what constitutes high and low, and yet another problem is determining whether aptitude or motivation is more important or to what extent an individual must demonstrate both.

High Skill High Motivation	High Skill Low Motivation
Low Skill High Motivation	Low Skill Low Motivation

Figure 1. Skill vs. Motivation

3.3 Content Analysis

> Content analysis is a research tool used to determine the presence of certain words or concepts within texts or sets of texts. Researchers quantify and analyze the presence, meanings and relationships of such words and concepts, then make

> inferences about the messages with the texts, the writer(s), the audience, and even the culture and time of which these are part. (Busch et al., 2005)

By using this methodology in reference to interviews, articles, and books about and by hackers, identification of prominent skills, tactics, techniques, behaviors, personalities, and motivations of hackers is possible.

According to Busch et al., there are two types of content analysis, conceptual and relational. For the purposes of this thesis, the appropriate method is conceptual analysis – "… establishing the existence and frequency of concepts…" (Busch et al., 2005). Busch et al. identify eight steps for a conceptual content analysis. Following are the steps as identified by Busch et al. The explanation of each step is in relation to its use in this specific document. Significant deviation and conscious decisions to deviate from the Busch et al. methods are noted.

1. Decide the level of analysis.

This research was not limited to single words or phrases. The coder decided on a case-by-case basis if a single word or a phrase provided the best meaning.

2. Decide how many concepts to code for.

Although Busch et al. recommends determining the number of categories before beginning the reading, this situation dictated an initial read of many of the articles to extract words, phrases and concepts that were used to create categories that seemed logical and appropriate for the context. Bush et al. recommend establishing the concepts before beginning to aid the researcher in looking for specific concepts and stay on task. However, they do note that flexibility in the number of categories is acceptable because it

allows the researcher to identify concepts previously undetermined but possibly useful. Once the categories were established, they were used by both coders.

3. Decide whether to code for existence or frequency of a concept.

Coding for frequency means that every time a word or phrase is used, it is tallied. Coding for existence, in contrast, means that once a word or phrase is used it is noted and there is no tally of how often that word or phrase was used. This research is based on the frequency of noted skills and motivations. The frequency of words, phrases or concepts should indicate how important that skill or motivation is for computer hackers. For example, if ten hackers identified programming as an important skill, that is taken much more seriously than if only one hacker identified programming as an important skill.

Frequency coding in this research comes with a caveat. The skill or motivation that was mentioned by a hacker was only counted once for each hacker's mention of it. For example, if an interview of one hacker repeatedly refers to programming as important, programming is only counted once for that hacker.

4. Decide on how you will distinguish among concepts.

This step required the coders to judge the concepts on a case-by-case basis. Coders were provided a list of categories and descriptions of those categories (see tables 1 and 2 for specifics). However, each coder was required to use his/her best judgment on the meaning depending on the context of the word or phrase.

5. Develop rules for coding your texts.

Since content analysis is a qualitative research method, it is important to establish and follow clear guidelines to improve the validity and reliability of the results. Specific

rules were provided to each coder as described later in this chapter. These rules provided to coders ensured each coder approached the literature the same way as the others.

6. Decide what to do with irrelevant information.

"The next choice a researcher must make involves irrelevant information. The researcher must decide whether irrelevant information should be ignored (as Weber, 1990, suggests), or used to reexamine and/or alter the coding scheme" (Busch et al., 2005). In this research, the coders were reading for specific motivations and skills as set forth by the guidelines. The other category for skills and motivations were used to classify skills and motivations that were not otherwise indicated.

7. Code the texts.

For this project, all coding was performed manually. This manual coding allowed the coders the leeway to eliminate redundant terms as predetermined by rules and use the context to code terms. The drawback of this method is that it leaves room for human error. A researcher could miss a term, count it more than once, misinterpret the context, or encounter numerous other problems. To mitigate this potential problem, the coder can highlight or in some way identify words already coded and label them with the appropriate code. Other solutions for mitigating some of these potential shortcomings are discussed later.

8. Analyze your results.

"Once the coding is done, the researcher examines the data and attempts to draw whatever conclusions and generalizations are possible. … Furthermore, given that the conceptual analyst is dealing only with quantitative data, the levels of interpretation and generalizability are very limited" (Busch et al., 2005).

Based on these guidelines, some of the specific instructions for this project included disregarding statement in abstracts or conclusions because those ideas are in the body of the article. The coders had to use his/her best judgment when descriptions within one article were repeated. The judgment was determined greatly by the context. The coder was not to count the same descriptions more than once if it was used by the same author and described the same person or event. For example, if an author described a hacker as a programmer once, it was tallied and then future references to the same hacker as a programmer were dismissed. Another restriction regarded descriptions or definitions. For example, if a term such as social engineering was recorded, words used to describe what social engineering is or consists of were not counted.

To form a list of traits, motivations, and skills that hackers have, claim to have, or exhibit, it was necessary to complete a content analysis of the literature relating to hackers. The list was developed from specific phrases or words in 21 different articles. Many of the authors used direct quotes from interviews with hackers or from hacker chat rooms or hacker publications. Once the list of terms and phrases were compiled, they were sorted into classifications to accomplish a frequency analysis.

The limitation of this analysis is that many of the authors refer to their own previous works and many cite the same studies and the same authors. These similar references cause content to be the same or very similar. To account for this duplication, if an author referenced the same interview or situation in more than one article, the words and phrases associated with that situation were only counted once.

Another limitation is that the categories were created by one researcher. A different researcher may have concluded more, fewer, or different categories. Human

error is always a potential problem. Humans make mistakes. In this case, words or phrases could be coded incorrectly or missed or duplicated. This potential problem was mitigated by using an additional reader. The additional reader was provided the exact same instructions and tools to code the literature. Another limitation was the lack of available literature and the relevancy of old literature. To mitigate this limitation, the researcher attempted to find the most recent articles written by recognized and professional authors on the subject. Using recent articles by professionals in the field should suggest that these articles include expert and comprehensive summaries of previous literature; therefore, without reading all the previous works, the researcher can obtain relevant data from the past and focus on the skills and motivations of contemporary hackers.

The initial read of the literature produced a list of adjectives and phrases that described hackers, their motivations, characteristics, and skills. This list generated an initial hypothesis of what types of people hackers are and what skills are necessary for this type of work. Based on these findings, categories were identified. These categories were used to identify the skills and motivations of hackers. These categories were used by the initial researcher to code the literature and the categories were provided to the additional coder.

3.4 Test Development

"Although there is no single correct way to construct a test, measurement experts generally agree that a systematic approach will most probably result in an instrument

with sound psychometric properties" (Bridge, Musial, Frank, Roe, & Sawilowsky, 2003). In order to make recommendations for developing a test, it is first important to understand how to develop a test. Here, two related methods are discussed and the recommendations in Chapter IV are based on these methods.

Downing and Haladyna provided the following table that describes the steps for creating item validity in test development.

Model of Item Validity Evidence: Qualitative Evidence

Type of Evidence	*Activity*	*Evidence Needed*
Content definition	Role delineation, job-task analysis; practice analysis completed	Documentation of the method(s) used to select item content
Test specifications	Table of specifications or test blueprint created	Documentation of systematic link of test content to test specifications or test blueprint
Item writer training	Develop training materials and methods; train item writers	Documentation of methods, principles, written materials, and sample items
Adherence to item-writing principles	Standard item-writing rules adopted	Evidence of compliance with rules and documentation of process used to review items
Cognitive behavior	Cognitive classification system used to classify items	Documentation of system used and its rationale; reports of any research using system
Item content verification	Content experts review and judge items	Content experts' credentials; records of content-expert review process
Item editing	Review items and professionally edit	Credentials and experience of editors; editorial and style guidelines, documentation of edit and review cycle
Bias–sensitivity review	Bias–sensitivity review policies and procedures developed	Documentation of bias–sensitivity review; rationale for policies; credentials of reviewers
Item tryout and pretesting	Pretest, pilot test, or field test items; item performance data; examinee interviews	Documentation of examinee pilot test data; examinee and item characteristics
Key validation and verification	Correctness of keyed answer verified by panel of content experts	Policy and procedures for key verification; documentation of key validation results
Test security plan	A test security policy and set of procedures are developed	Copy of policy and procedures manual that specifies how items are protected from security lapses

Figure 2. Evidence for Item Validity (Downing & Haladyna, 1997**)**

Downing's and Halayna's first step is content definition. They recommend different ways of performing this, but as already noted, the cyber warriors' tasks are still undetermined. Some representative tasks, therefore, will be identified from the content

analysis. The next step, test specification, is addressed in the next section that describes test blueprints in more detail. As noted, the Air Force does have an organization for test development. It is also possible that some of the content experts, once identified, may have some experience in this area. If not, there is training is available. With training or experience, writers should be able to apply the item-writing principles they know and document those steps, or request the Air Force organization to provide guidelines to follow. The cognitive behavior is also addressed in the blueprint method that follows. Item content verification is difficult at this time because it should be completed by content experts. When content experts are identified, they can verify and/or change items. Item editing will include scrutinizing the test for grammar, style, and format consistency. Bias-sensitivity review should be conducted by the Air Force test-writing professionals or someone trained in this specific area to ensure biases do not exist. Item tryout and pre-testing can be conducted in many ways. The Air Force has an abundance of personnel at multiple locations and with varying levels of experience and training. By leveraging its resources, the Air Force can perform this step with little difficulty and receive very useful feedback. For example, the test could be given to AFIT students in different programs and also to enlisted trainees at technical training schools. These two demographic situations should provide very useful information regarding the difficulty of the test and the level of training and education needed to do well on a test. There are other options within the Air Force as well. Tests could be sent to squadrons or other training and educational environments. There is no shortage of options to meet this requirement. Although the final two steps should be relatively easy and self-explanatory,

they should not be overlooked. The following table provided by Downing and Halayna is a way to verify all the above steps have been completed.

Qualitative Evidence For Item Validity

1. How is the content of the examination defined? Was a job-task analysis carried out? Was a practice analysis carried out? How were the content expert judges used during the process of defining test content?
2. Have item cognitive classification guidelines been developed based on a content analysis of what the examination is designed to measure?
3. Do these guidelines contain a classification system for the type of cognitive behavior or other systematic method of classifying type of behavior to be measured by the item?
4. How is the item content systematically related to the test specifications? Is there documentation relating item content and test specifications?
5. Is there evidence of consistent classification of item by content domain and by cognitive behavior?
6. Are item writers qualified based on their content expertise?
7. How well have item writers been trained to the task of item writing?
8. Have items been edited according to written editorial guidelines?
9. Are item editors qualified for this task? What is the experience of the editors with respect to test item editing?
10. Is there an adequate test security plan emphasizing security throughout the test development process?
11. What evidence exists that test security has not been breached?
12. Have guidelines been established for item bias–sensitivity review?
13. How were bias–sensitivity reviewers trained for this task? What are their credentials for this task?
14. What are the results of the item bias–sensitivity review?
15. Has the scoring key been validated by a consensus of experts in the field using all empirical data available?
16. Have the test items been subjected to a review of their adherence to well-established item-writing principles? Has item relevance to the field been reviewed and documented?

Figure 3. Item Validity Verification (Downing & Haladyna, 1997)

The blueprint method offered by Bridge et al. is part of the *test specifications* and *cognitive behavior* activities as cited above. This method is not as formal or well structured as Downing and Haladyna but with the two methods used simultaneously, test validity and reliability should be ensured.

Bridge et al. identify their four steps to developing a content-valid test:

1. Ensure the test has an established purpose for its intended use and the test is actually measuring what it purports to measure.
2. The test items should sample the domain of interest and reflect proper proportions of importance.
3. Test items must be clearly written and of high quality.

4. Have experts in the field review the test blueprint and table of specifications, as well as the quality of the items that have been developed for each content area. (Bridge et al., 2003)

To aid in following their steps, they offer an example of the blueprint and table of specifications, a task analysis form and an item specification form. This example is provided in Figure 4. The example indicates how the blueprint and table of specifications would be developed for a test based on evidence based medicine (EBM). Although the content of this example is in no way related to the topic of interest in this document, it is a valuable visual aid because it shows how to use this method for a variety of subjects or tests. The blueprint and table of specifications exist on the same document as seen below and meet the requirements of steps 1, 2, and 5 from Downing and Haladyna. Panel 1 is the test blueprint. The content areas are derived by the content definition task as suggested by Downing and Haladyna. The second column in panel 1, *% of items on test*, should reflect the "amount of time spent on each competence" (Bridge et al., 2003). Here, Bridge et al. are referring to the amount of time spent in class, but for the purposes of an aptitude test, this could indicate the ratio of test questions dedicated to a specific content. Higher percentages would indicate specific content areas that are more important or more relevant than the lower percentages. Panel 2, the *Table of specification levels*, relates directly to step five of the Downing and Haladyna method. Bridge et al. cite Ward's cognitive taxonomy. This taxonomy has three levels, recall, application, and problem solving. If test makers determine more levels are necessary, this table can easily be adjusted to reflect Bloom's taxonomy that has six levels: knowledge, comprehension, application, analysis, synthesis, and evaluation (Clark,

2001). This panel indicates how many questions in each content area are at a specific cognitive level. This is important because there is a big difference in knowledge

Panel 1		Panel 2		
Test blueprint		Table of specification levels		
Content area*	% of items on test **	Recall %	Application %	Problem Solving %
1.0 Principles of Evidence Based Medicine 1.1 EBM defined 1.2 Why practice EBM 1.3 How to ask appropriate questions in EBM 1.4 Where to search for answers 1.5 Strengths in the different sources of evidence 1.6 Bias and random error	20%	20%	0%	0%
2.0 Evaluating Risk 2.1 Pretreatment risk 2.2 Probability and odds 2.3 Incidence and prevalence 2.4 The 2 x 2 table 2.5 Relative risk **2.6 Odds ratio**	15%	10%	5%	0%
3.0 Interpreting Test Results 3.1 Sensitivity and specificity 3.2 Likelihood ratio 3.3 Positive and negative 3.4 Confidence intervals	25%	5%	10%	10%
4.0 Treatment Effects 4.1 Risk reduction 4.2 Benefit increase 4.3 Risk increase	15%	5%	10%	0%
5.0 Using Evidence in Medical Management Decisions 5.1 Clinical decision analysis 5.2 Values and preferences of patients and populations 5.3 Costs/economic analysis	25%	5%	15%	5%
Total	100%	45%	40%	15%

Figure 4. Blueprint and Table of Specifications (Bridge et al., 2003)

and skills of someone who, for example, knows the names of ports and protocols and someone who understands and can exploit the weaknesses of ports and protocols. This

analysis can be used to indicate at what level of understanding an applicant is and may be used to classify them into different training and education courses.

Although Bridge et al. describe the task analysis form usefulness in academic terms of prerequisite skills, enabling skills and competence; this is directly transferable to the military setting. The EBM example from Figure 4 is continued in Figure 5, the Task Analysis Form. The form identifies a competence from the test blueprint and provides a brief description. In an academic setting, *Prerequisite Skills* would "…represent material taught in previous sessions or the previous term" (Bridge et al., 2003). In the military setting, it would indicate skills or knowledge that the applicant must already have to demonstrate the subsequent skills. In the military, there is no difference if the skill or knowledge was formally taught or when, it is just important to identify the applicant already has this knowledge or skill. Number four identifies enabling skills. "Enabling skills represent the key steps that take the student from prerequisite skills to the final competency" (Bridge et al., 2003). Number five is demonstration of the specific competency. Obviously, these relate to the cognitive abilities previously addressed. Therefore, if additional cognitive levels are added, the task analysis form may have to be adjusted according.

Figure 6 continues the EBM example. The item specification form is created for each test item and consists of five components. The first two components come directly from the test blueprint. "The third is the stimulus characteristics, which set the structure of the question" (Bridge et al., 2003). This may be described as the content of the stem of the question. "The fourth criteria comprises the response characteristics, which denote the allowable formats for an acceptable response, as well as the distracters that will be

used. The final step is to construct sample items, which are scrutinized and compared with the test blueprint, table of specifications, task analysis and item specifications" (Bridge et al., 2003).

Task Analysis Form

1. Competence ID No: 2.6

2. Topic Description:
Computing an Odds Ratio
_____
_____
_____

3. Prerequisite Skills:
- Multiplication
- Division
- Definition of exposure
- Definition of disease
- Definition of risk

4. Enabling Skills
- Creating a 2 x 2 table
- Labeling quadrants
- Providing a formula

5. Competence
- Odds ratio less than 1: (a/b) < (c/d)
- Odds ratio equal to 1: (a/b) = (c/d)
- Odds ratio greater than 1: (a/b) > (c/d)
- Interpretation of odds ratio

Figure 5. Task Analysis Form (Bridge et al., 2003)

Although time consuming, the two methods used together provide the guidance and tools necessary to create a valid and reliable test. Crucial to valid and reliable test is the content and content experts. Without these yet determined, the Air Force will have to determine other ways to meet these specifications. The content method proposed here is to use the skills and motivations of computer hackers as determined by the content analysis in the next chapter. Although content experts are not yet formally determined in the Air Force, the content suggestions provided here will help in determining what people

already poses those skills and knowledge and those individuals can be used as the experts until more about cyberspace warriors and their jobs are determined.

Item Specification Form

1. *Competence Number*: 2.6

2. *Competence*:

Evaluating Risk: Odds Ratio

3. *Stimulus Characteristics*

The stimulus will describe data from a case-control study, from which students will be required to determine the odds ratio solution and apply the rule to the associated problem (taxonomy = problem solving because the solution strategy and formula are not given).

4. *Response Characteristics*

A. Examinees will be able to choose from five multiple-choice options with one correct answer.

The correct answer will be numeric and achieved by correctly calculating the odds ratio.

B. Two of the four distracters will be numeric and reflect the incorrect placement of the values in the 2 x 2 table. (e.g. a x b/c x d; b x c/a x d). One distracter will be a numeric value close to the correct answer, while the last distracter will be a 'none of the above' response.

5. *Sample Item*

A case-control study was conducted to assess the relationship between smoking and heart disease. Of the 50 *cases* included in the study, 40 were smokers. Of the 1450 *controls* included in the study, 460 were smokers. Estimate the relationship between smoking and heart disease?

(A) 18.60
(B) 9.20
(C) 8.60
(D) 0.12
(E) None of the above

Figure 6. Item Specification Form (Bridge et al., 2003)

3.5 Summary

This chapter presented the methodologies used in the research to identify the skills and motivations of potential cyberspace warriors and the methods used to critique

an existing test and suggest a new test. First, a literature review was used and yielded a quad-chart that identified the four skill and aptitude combinations and indicated which quadrants offer the best chance for success for cyberspace warriors. Although the quad-chart appears to clearly differentiate skills and motivations, it is important to realize that both actually exist on a continuum and it is difficult to say whether motivation or skill is more important. The content analysis method was also explained. This method has been used to analyze the content of words and phrases (Busch et al., 2005). For this research, the content analysis is used to determine what skills and motivations computer hackers have through the conceptual analysis method of content analysis. Finally, two methods of test development were described. These methods work in conjunction to ensure a reliable and valid test is created. Some of the challenges facing the development of a cyberspace aptitude test were noted. Chapter IV will use the results of these methodologies to propose what a cyberspace aptitude test should be and compare this to an existing test.

IV. Results and Analysis

4.1 Introduction

This chapter presents and discusses the findings of the literature review, the content analysis, the test critique and recommends how to improve tests or develop a screening process based on the findings of the content analysis. First, the literature review will be analyzed to facilitate discussions regarding the emergence of a command and the selection of cyberspace warriors. Second, the results of the content analysis is presented including a discussion regarding how realistic and usable the findings are. Third, the pros and cons of using an analysis based on civilian individuals performing illegal activities to determine the skills and motivations for military use are discussed. Fourth, a comparison of the findings to an existing test is presented with critiques of the test and suggestions for improvement. Finally, a proposal for a new screening method is provided. This proposal will include specific content, quantity, and cognitive level distributions.

4.2 Literature Review Analysis

The literature revealed that concerns for protecting and defending the U.S. technology dates back to the 1970s. Since then, our society has become increasingly dependent on technology and particularly the realm of cyberspace. As cyberspace has surfaced as an economic, social, and political center of gravity, it is only natural for it to also become a military domain. Currently, the thoughts regarding the use of cyberspace

have expanded from defending it to using it as a domain in which adversaries can be attacked. Flying and fighting in cyberspace implies defending our own cyberspace and infiltrating and exploiting the adversary's cyberspace. There is a long-standing acknowledgement that the United States is especially vulnerable to a cyberspace attack because of our commercial, public, private, academic, and military dependence on cyberspace. However, until recently, the military has not publicly acknowledged the use of cyberspace as a specific mission. The Air Force has accepted the challenge of this mission and is working hard to resolve the many issues accompanying the new mission.

One of the paths the Air Force is taking is to develop a command dedicated to the cyberspace mission. To assist, different organizations have been tasked to support the development of the command in one way or another. The Air Force Institute of Technology hosted a workshop to begin defining education and training requirements for a cyber force. A large part of this task is to identify what competencies cyber warriors must have, or what tasks they will be expected to accomplish. That is a daunting challenge but the group was able to identify competencies for network operators based on some of their stated assumptions. They identified positions, and the general competencies and experiences required for each position, and they were also able to provide very specific competencies and experiences for some positions (Cyber Forces Education and Training Workshop - 1st Quarter CY2007, 2007). As a precursor to training and education, the military must recruit those with a high potential for success in mastering those competencies. Testing is the method the military has successfully used to screen potential candidates for decades. As a proven method, there are no grounds for altering this method. As long as the tests can be adjusted to include the appropriate

aptitudes for cyberspace warriors, testing should prove useful. However, testing is not the only option and it certainly is not a panacea for filtering candidates. Just as with pilots, initial testing, follow-on testing, and continuous assessment can be used to continuously filter personnel. The U.S. Air Force pilots are arguably the best in the world. One contribution to their success is the screening process used to filter out those that are unlikely to be successful. Once again, this method is working; therefore, with caution, it can be applied to a different occupation, and if used correctly, should aid in the selection of successful cyberspace warriors.

4.3 Content Analysis Results

The articles and books were analyzed by the criteria set forth in Chapter III. Readers were looking specifically for words and phrases that indicated the motivations hackers have for performing hacking and the skills hackers use to perform their tasks. These two components form the basis for the considerations in selecting cyber warriors. Eight categories each were created for both motivation and skill. This breakdown provides the foundation for the types of questions that should eventually be on a test or what types of skills and motivations an evaluator should observe in applicants. The evaluations of the 21 articles are provided in tables 1 and 2.

Table 1 identifies the different motivations, provides a definition of each motivation and indicates how many instances of that motivation were found by each reader (R1 indicates reader one, and R2 indicates reader two) according to the guidelines as set forth in Chapter III.

Table 1. Hacker Motivations

Title	Description	Instances	
		R1	R2
Quest for knowledge	Desire to learn more about hardware, software, architecture, programming, or any associated skill.	38	25
Financial/personal gain	Desire to make money or prevent others from making money	23	21
Power/status/ego	Desire to gain respect and demonstrate skills to peers or the opposition. The need to feel better about oneself.	27	20
Social/political/moral reasons	To influence others or spread information about a cause or to warn others about something the hacker and/or his/her organization feels strongly about or what they stand for.	30	26
Obsession	Compelled to hack, an uncontrollable urge.	6	5
Fun/challenge	Something the hacker enjoys doing.	23	23
Sense of community	Desire to feel like one is part of a community, sometimes an elite community.	22	8
Other	Revenge, espionage, lack of consequences.	27	25

The Hacker Motivation Table (Table 1) demonstrates how varied hacker motivations are. One of the interesting findings is the lowest category is *Obsession*. The low values in this category indicate that although a few hackers do feel obsessed, most do not. Obsession with any activity is unhealthy, therefore this low number is positive. The next lowest motivation is *A sense of community*. This motivation is one the military can support and should encourage within its ranks. Hackers are very social within their own community. "…contrary to their popular mythology, hackers often hack in groups, both in the sense of physically being in the same room while hacking and of hacking separately but being in a group that physically meets, that frequents bulletin boards, online places to talk, and that exchanges e-mail" (Jordan & Taylor, 1998). These communities serve two primary purposes. One purpose is to socialize and the other is to

help each other. Hackers have different specialties. When they work together they can leverage each others' knowledge and are more likely to successfully complete their intended hack. The advantages of this type of community are very valuable to the military. The next category is *Financial/personal gain*. Although this category may appear to be contrary to military values, this motivation could still be worth testing. The existence of this motivation might be useful to exploit in other ways. For instance, bonuses or promotion opportunities could be dangled as motivators. Learning these skills and gaining experience will be useful for future jobs in the civilian community. The next highest category is *Fun/challenge*. This is important as it suggests "… the simple argument that to do what you do well, you must be enjoying what you do" (Herrington, 2004). This category indicates that there are many in our society who will enjoy doing this type of work. If the military can find and employ these individuals, it will be a win-win situation for the organization and the individual. The category of *Power/status/ego* is the next highest cited category. High scores in the category demonstrate that not only do hackers enjoy what they do, but also they view hacking as some type of competition and they strive to do better for themselves and to prove to others that they can. This sense of competition is useful in the military setting. The military is based on competitive nature as demonstrated through the promotion process. All military candidates should have some desire to continually achieve more and improve oneself. A test for cyber warriors would have to identify this in the particular domain of computer related activities. The next category for consideration is *Social, political, and/or moral reasons*. This indicates that people who believe in a cause and believe that computers are a way to promote their cause are highly motivated to acquire the skills and spend the time associated with

learning about computers and networks. The military is filled with troops who believe in the United States and our way of life. This type of motivation may be used to encourage some to improve their skills or it may be used to recruit skilled computer operators. Conversely, it could be a downfall because people that are already in the military or who are joining do so because of their belief in our country and our way of life. Quest for knowledge is a highly cited category. It is based on improvement but specifically knowledge in this field. Hackers seem to have an inherent desire to continually learn more about hardware, software, applications or any aspect of computers. This is a good trait to have because computers change and new skills must be learned and practiced to keep up. Raymond recognizes the dynamic world of hacker skill sets, "This toolkit changes slowly over time as technology creates new skills and makes old ones obsolete" (Raymond, 2006). The sense of community is another dominant motivation for hackers. "The original hacker stereotype is a smart, lonely deviant — a teenage or adult male who's long on computer smarts but short on social skills. But like most stereotypes, it doesn't begin to tell the whole story" (Bednarz, 2004). The category titled *Other* deserves special consideration. It consists of motivations that are not closely associated to any of the other identified categories, but are not cited enough to warrant their own category. Some of these motivations include doing something illegal just to do it, escape from reality, to cause harm, lack of consequences, the anonymity of it, because it feels good, or because they are bored (Jordan & Taylor, 1998). Another noteworthy reason not often cited is because "[Hackers] want to help system managers make their systems more secure" (Denning, 1990).The high value associated with the *Other* category indicates that there are many reasons people are motivated to pursue this activity. For the Air Force to

leverage this knowledge, they will have to determine which motives are congruent to the Air Force values and select individuals that are motivated to do these activities for reasons the Air Force believes are acceptable.

Table 2 identifies the different skills, provides a definition for each category and indicates how many references to the respective category were found by each reader (R1 indicates reader one and R2 indicates reader two) according to the guidelines as set forth in Chapter III.

Table 2. Hacker Skills

Title	**Description**	**Instances**	
		R1	**R2**
Programming	Knowledge about and ability to use computer languages. This may include writing code, examining code, debugging code or inserting bugs into code.	16	16
Network and security knowledge	Architecture, ports, protocols, and the associated weaknesses and strengths.	15	21
Problem solving	The way a person approaches a problem. This may include organization, logic, reasoning, or method used.	9	4
Social engineering	A method of deception. Gaining information or access by impersonation or playing on the natural inclination of people to help others.	2	3
Software/application knowledge	Ability to use worms, trojans, email viruses, and/or hack websites. This skill is differentiated from developing or programming.	7	18
Other	Skills not otherwise covered such as dumpster diving, distributing pirated software and property, gather information about networks, companies, or individuals.	1	6
Hardware	Knowledge of how to build hardware or associated vulnerabilities.	4	4
Cryptography/authentication	Knowledge regarding the use of encryption and decryption methods. The ability to manipulate, use, or circumvent authentication techniques.	8	5

Some of the differences between the reader results indicate that these categories are closely related. For example, what one reader considers cryptography, another may

consider the ability to use software that assists with circumventing authentication. The way the reader codes it will depend on his/her interpretation and/or his/her previous experiences. What the results of this analysis indicate are that there are several skills necessary to perform hacking activities and they are not mutually exclusive. Some of the skills may be considered a lower level, but mastery of the lower skill promotes learning the next. For example, compare the *Software/application knowledge* category to the *Programming* category. The ability to use worms, trojans, hack websites, etc is a low level, but necessary skill. This category indicates an ability to use an existing vulnerability but does not indicate the intellectual prowess to write a program or evaluate text to exploit a vulnerability. Because of the preponderance of websites with viruses, worms, etc., hackers do not have to do much but download and run tools that exploit a vulnerability they choose. Programming indicates a higher level of knowledge and experience with computers and the way they work and respond. This skill indicates the ability to write, read, and understand at least one computer language. This skill allows the person to create his/her own programs as ways to exploit computers and computer systems. Just as some of the skills help the advancement of another skill, some skills are similar to each other. A good understanding of one category contributes to knowledge in others. *Software/application knowledge* indicates knowledge of how to use exploits. *Network and security knowledge* refers to knowing the ports and protocols used throughout the network along with security features and devices such as firewalls and routers. Architecture refers to understanding how the hardware is connected physically and logically, how the applications work together and the ports and protocols in use. These three categories are closely related and knowledge in one assists with

understanding and learning in the others. Cryptography is primarily based on math skills but this category also includes an understanding of the different types of cryptography, how they work and under what circumstances one is used. Problem solving is also a necessary skill. This includes logical thinking and creative thinking. When hackers are confronted with a wall, sometimes they find a way through the wall, but many times, they find another way around it. Social engineering is a skill that may or may not include technical computer skills.

> Social engineering is the hacker term for a con game: persuade the other person to do what you want. It is very effective. Social engineering bypasses cryptography, computer security, network security, and everything else technological. It goes straight to the weakest link in any security system: the poor human being trying to get his job done, and wanting to help out if he can. (Schneier, 2000)

The final category regards knowledge of hardware. This could include building or dismantling, knowing how hardware connects or knowing what the strengths and weaknesses are. The low instances of this category are representative of the evolution of software. Hardware is not usually associated with weaknesses or vulnerabilities anymore. The few instances of other indicate that this list encompasses most of the necessary skills of hackers. It is important to note that these skills will evolve and change as technology evolves and changes. The Air Force must always be cognizant of the changing skill sets necessary for potential cyber warriors and adjust selection methods and training accordingly.

4.4 Content Analysis Discussion

It is easy to imagine how effective a highly motivated and skilled hacker may be. Multiply the effectiveness when two or more highly motivated hackers work together towards a common goal. If they compliment each others' strengths and weaknesses, the possibilities are endless. This possibility is what the Air Force needs to exploit. With the known skills and motivations of hackers, the Air Force can devise screening methods to recruit those with these skills and motivations to work as cyberspace warriors. The categories here are broad but do provide a start. To write test items, a further breakdown of the categories is necessary. It is also necessary to write questions at different cognitive levels to differentiate the level of knowledge candidates poses.

Written tests are not the only option for a screening process. Performance tests can provide an assessor even more valuable information than just a test. Candidates can be given a computer and a scenario. In the scenario they are required to perform certain actions using the computer. These activities can be timed, assessed by the use of available resources, or by the different methods by which they complete the task. Another possibility is to have candidates attempt to penetrate a network. The assessors could watch on honeypots or intrusion detection systems and defend the network upon detection. Then the candidate can respond to the detection. Tests that are similar to actual working conditions allow assessors to watch how candidates perform under pressure and if planned and conducted correctly, can demonstrate how they work with others and how they react to situations.

There are some concerns about profiling civilian individuals who perform activities and then using that information to recruit individuals for work in the military. "It makes sense that security professionals tend to come from the hacker community,

since a typical hacker is well educated in the common and not so common doorways that companies inadvertently leave open into their inner sanctums" (Mitnick & Simon, 2005). However, the individuals the military recruits for these activities should not be convicted criminals and will be screened according to standard procedures. This study proposes considering what hackers do and why and using that information to select individuals with a prowess for this work. Eventually, those selected will perform activities similar to those of hackers, but the military members will do it in accordance with proper military guidance and approval.

4.5 Critique of 315 IOS Test

The 315 Information Operations Squadron (IOS) is an Air Force organization whose mission is to "Conduct computer network attack (CNA) when tasked to satisfy Combatant Commander's requirements. Conduct computer network exploitation (CNE) when tasked by the National Security Agency to achieve CIA, Secretary of Defense, and Combatant Commander Intelligence needs" (Robinson, 2007). They are one of only a few organizations that have the capabilities, personnel, or training necessary to perform such a mission. In order to complete such a unique mission, the 315 IOS has found it necessary to be selective with their personnel. To screen candidates, they have implemented a screening process that consists of a test and an interview as described below.

The 315 IOS devised an assessment they require potential workers to take. The test contains two parts. If the applicant's test results are good – (75% or higher on the

multiple choice) the candidate is further screened with an interview. Part one of the test consists of 89 multiple choice questions concerning TCP/IP, computer network fundamentals, UNIX commands, and intrusion detection. Part two consists of open-ended questions regarding personal experiences with computers. The interview is used to expand on part two of the test and allows the interviewer to get a better sense of the candidate and if he/she will fit into the organization.

The 315 IOS designed this test because of their unique, new mission and because they could not find an existing test to meet their needs. They prefer applicants with some military experience rather than new military members fresh from technical training. Technical training is usually behind on new technologies and techniques that the 315 IOS may use. They are also concerned that young troops do not have the maturity level and respect for the outcomes of this type of work.

The results of the content analysis provided a comparison tool for the 315 IOS test. The first critique is in relation to the types and varieties of questions of the 315 IOS test compared to the content analysis results. The second critique evaluates the cognitive level of the 315 IOS. Finally, recommendations to improve the test are provided.

Part one of the 315 IOS test is focused on the technical knowledge regarding the previously stated subject areas. When attempting to compare these questions with the categories obtained in the content analysis, the discontinuity is apparent. The test is very academic. It focuses on terminology and academic labels such as the Open System Interconnection basic reference model. The literature revealed that hackers do not appear to worry about the definitions and labels academia places on practices, theories, or techniques. Although this is important because it demonstrates a basic level of

understanding and demonstrates at least some level of education or training, this is not enough. Vocabulary is at the lowest end of Bloom's taxonomy and can therefore be taught and learned easier than tasks. Certainly this conclusion does not indicate that a screening test should disregard jargon. When working in a military setting, a common vocabulary is critical; however, this conclusion denotes the importance of screening candidates in a way they can demonstrate their skills not just demonstrate their ability to define words. The test also focuses only on UNIX. Although knowledge of UNIX is useful and necessary, there are many other computer network topics to consider, and according to Raymond, hackers, and therefore cyber warriors, "need to learn how to think about programming problems in a general way, independent of any one language" (Raymond, 2006). Another critique is that most of the test is devoted to what the content analysis classifies as network/security knowledge. This is inconsistent with the findings of the content analysis. A test for cyber warriors should include a large portion regarding knowledge and application of worms and viruses and exploiting vulnerabilities along with a variety of languages, problem solving techniques, architecture, and social engineering. The test is written from a defender or security perspective. Until recently, defense of the military networks and infrastructure has been the primary mission of computer professionals. Although defense remains an important part of the mission, "Good security was never more important than in a world populated by terrorists" (Mitnick & Simon, 2005) the military must assume a more offensive position and tests should reflect this new perspective.

Most of the test is written at the lowest of cognitive levels. According to Bloom's taxonomy, the questions are considered at the knowledge level, which is simply restating

information (Clark, 2001). Although important, potential cyberspace warriors must demonstrate an ability to do more than regurgitate facts. The test lacks a way for a candidate to demonstrate higher levels of cognition that are very important for cyberspace warriors. Simply knowing what ports and protocols are associated with what services does not make an individual qualified to undertake some of the responsibilities and tasks that will be required of a cyberspace warrior. Part two may attempts to compensate for this failure through its use of open-ended questions. Although these questions address experience they do not offer the candidate an opportunity to demonstrate his/her skills. There is a huge difference in knowing what a buffer overflow is and actually using that vulnerability to cause a desired effect.

4.6 Recommendations Based on Findings

Although the 315 IOS test has been somewhat useful for their purposes, a more comprehensive selection process will likely increase the success rate of hiring the right people for cyberspace operations. As cyberspace operations develop into standard practice, career fields, career paths, and positions will emerge. Cyberspace units will not need to screen candidates because the selection process will be similar to that of any other career field. Before cyberspace operations are normalized, it is critical to identify what predicts success for these operations and develop a standard screening method to ensure the right people are selected and trained for established cyberspace positions. "Once we know the attributes of employee success, we can name the employee specifications required for the job. We can measure applicants with respect to these

specifications and make our predictions accordingly" (Gatewood & Feild, 2001). The current problem is the specifications are unknown. The content analysis is an approach for identifying the necessary specifications. All cyberspace warriors must have some basic understanding of all the subjects and how they work together.

Cognitive levels assessed and methodology should be determined by the objective of the test. If a test is provided to enlisted candidates, such as during the ASVAB, then the cognitive level tested will presumably be towards the low end of Bloom's taxonomy and the method will be multiple choice to fit the current format. A test at the knowledge level is used for significantly different reasons than a test at the synthesis level.

Candidates should be questioned regarding their motives to become a cyberspace warrior. According to the content analysis, the most important motivation is someone who wants to do this work for enjoyment. This enjoyment may stem from the challenges that computers and networks pose or simply the joy of working with computers. Certainly, some people prefer to interact more with computers than with other humans. The rise in popularity of computers in gaming and socializing demonstrates that our society is becoming more comfortable with computers and that people enjoy the time they spend on computers.

The second quality expected for good candidates will be a strong moral belief in what he/she is doing. These types of questions could include dedication to the organization and patriotism. The problem for this type of motivation is that in the military setting, this quality should be predominant. Today's military is an all-volunteer force that indicates people are there because they want to be.

The third motivation of power, status, and/or ego may initially seem like a motivation the military would not desire. However, the desire to outperform peers and demonstrate ones skills over another are actually coveted by the military. Competition breeds ingenuity and promotes perpetual self-improvement. However, these motivations must be coupled with an ability to work with a team and take orders from superiors. Determining a candidate's quest for knowledge is also an important factor. This implies a more altruistic motivation but is closely related to the motivations of fun and power.

Recommendations for a screening process include tests that are not necessarily multiple choice, essay or pencil and paper. A good test for cyberspace operators should place them in a realistic situation. For example, candidates could be given a scenario and the tools they need to complete the mission and then given free reign on execution. Another option is to place a candidate with a team. The team would be composed of some of the different specialties the candidate will be expected to work with in a real situation. Then the team is given an objective and observers can score the candidate on his/her specific skills and the ability of the candidate to work with the team.

The type of test, the cognitive level assessed, and the setting in which the test takes place depends on the objectives. The actual test level and intensity will vary. If the intent is to identify those with the basic knowledge of networks, ports, protocols and languages, something similar to the 315 IOS test is very valuable. This test assumes the candidate will receive follow-on training to better prepare him/her for actual operations. It also assumes that this type of technical knowledge is desired. This test does not evaluate problem-solving abilities, creative thinking abilities, communication abilities, all of which are important for a situation where new problems emerge daily and require

creative thinking to deal with the situation, such as in cyber operations. "Specific technical skills are easy to focus on but have an increasingly limited applicability. Aptitude to learn new technologies is more critical in the long run. To better implement this philosophy, organizations are encouraged to widen their applicant pools to include non-IT personnel and nontraditional workers" (Nelson & Todd, 2004).

4.7 Test Proposal

The culmination of this research is a proposed testing process. Although specific test items and therefore an actual test are not within the scope of this thesis, below are some proposals for the different types of tests that may be used in the near future. The recommendations are based on the content analysis results, the critiques of the 315 IOS test, and the previously discussed recommendations. The suggestions here are for technical and non-technical cyberspace warriors. The idea is to find people who have the ability and motivation to learn and succeed in this domain. Not all aspects of cyber operations, not even the networking portion, will be completely technical.

Questions regarding technical abilities should include general knowledge and specific knowledge. Individuals that possess an understanding of general network knowledge may be useful in planning while those with specific knowledge will be useful in executing the plan. Planners should have a big picture of what needs to happen to create an operational effect. With this understanding and a basic understanding of what specific skills exist within a cyberspace operations organization, this person will be able

to gather the individuals with the specific skills to create the effect. Both people are necessary to plan and execute the mission.

Multiple-choice tests are a very useful tool for mass testing purposes. The ASVAB and the AFOQT are the multiple choice tests the military uses for determining who is qualified and competent enough to enlist or be commissioned, respectively. These tests are also used to aid in career field assignments. Many career fields have minimum scores a candidate must meet or exceed in the different parts of the test. As already discussed, the military has found great success in this filtering method. Therefore, the addition of cyber aptitude questions or a cyber aptitude portion could be added to each as an initial filter for cyberspace warriors.

The ASVAB and AFOQT are only intended to test for aptitude. The premise of this thesis is that aptitude is not enough; motivation is also important. Therefore, an additional test must be implemented to screen for motivation in those that meet or exceed the minimum criteria for cyber warriors. As it is undetermined if motivation or skills are more important, the testing sequence appears to be of no importance. Therefore causing as little disturbance as possible to the existing testing process is recommended.

There are two concerns that must be addressed concerning officers. The first is that academy students are not required to take the AFOQT. Therefore, another selection process must be in place for these individuals. A possible solution is to consider their major. Decisions regarding what majors are useful in cyberspace operations could be used as a way to identify potential candidates. However, selection based on college major is actually the second concern identified here regarding officers. There is not a major for this career field. Certainly, it is possible to implement a track or educational

path that would lend itself to this career, but this path would be difficult to implement in institutions besides the Air Force Academy. Additionally, it is not always good to assume that just because someone completes a program he/she must continue into an AFSC that is similar.

It is also possible to implement tests that are not multiple-choice. Another test option could be scenario based. This type of test would be similar to exercises. The military does exercises to test processes, procedures, and see how people react in a stressful situation. This would be a useful tool for potential cyberspace warriors. Since this would require significant planning, this screening tool would best be used after other methods have screened those that appear to be likely to succeed in this environment.

4.8 Summary

This chapter analyzed the literature reviewed for this thesis. Then the results of the content analysis were presented and discussed. Using the results of the content analysis, a cyber aptitude test used by the 315 IOS test was critiqued. By using the content analysis results, the 315 IOS test, and the critiques of the test, recommendations for developing new screening tests were provided. The recommendations include a variety of screening methods from multiple-choice to scenarios based on the intent and level of the screening method.

V. Conclusion

5.1 Discussion

The purpose of this chapter is to discuss anything pertinent, but not covered in the previous chapters, to recommend follow-on research topics related to this topic, and finally, to state the overall conclusions of the thesis.

The research process brought to light many considerations regarding cyberspace warriors, cyberspace as a military mission, and the hacker community as a reference for skills and motivations. Because this research was centered on the belief that the skills and motivations of cyber warriors could be garnered from that of computer hackers, there was no suitable position to discuss them until now. Although these considerations are not directly in line with this research, they are worth considering. The ideas discussed here are not necessarily subjects to be researched, but they are ideas and observations worth noting.

One of the first noticeable Air Force deficiencies in cyberspace is the lack of doctrine. Because "…doctrine is an accumulation of knowledge gained primarily from the study and analysis of experience, which may include actual combat or contingency operations, as well as experiments or exercises" (Department of the Air Force, 2003). The doctrine cannot be written without experiences, experiments, and/or exercises. However, "It should form the basis from which Air Force commanders plan and execute their assigned air and space missions and act as a commander within a Service, joint, or multinational force" (Department of the Air Force, 2003). Obviously, with the

assumption of a new mission, Air Force doctrine must be reevaluated. Much of cyberspace doctrine can be adapted from existing documents from related fields such as information warfare. However, as the field becomes more defined and developed, policy and doctrine will need to be refined accordingly. A big challenge in this field is that technology advances quicker than policy or doctrine can be created, edited, and written. Hellion recognized the connectedness and importance of technology and doctrine.

> We must recognize that both technology and doctrine are dynamic processes, always advancing or receding, and are necessarily adaptive to change lest they stagnate and lose relevance. Neither is independent of the other; rather, each generates a synergistic impulse that encourages and strengthens the other. The lagging of one is necessarily injurious to the other. (Hallion, 1987)

Additionally, cyberspace is a current struggle for the Air Force. Although the Air Force has used the components of cyberspace, such as computers, networks, and the electromagnetic spectrum for years, it is a struggle to determine how to fight in cyberspace. Along with the challenge of determining how to fight in cyberspace are the challenges regarding the legal, social, cultural, and political ramifications of such warfare. The military must consider the laws of armed conflict and how they do and do not apply to cyberspace.

A concern regarding the methodology of this research is the ethical dilemma it poses. Civilian hackers perform illegal activities and this research is based on their skills and motivations. Certainly, their motivations may be questionable in reference to the Air Force morals. However, few will argue that they have the skills the military needs.

> I've heard lots of security lectures, and the most savvy speakers are the hackers. For them, it's a passion. Hackers look at a system from the outside as an attacker, not from the inside as a designer. They look at the system as an organism, as a coherent whole. And they often understand the attacks better than the people who designed the systems. (Schneier, 2000)

Therefore, the military must consider if recruiting individuals with questionable morals is worth the potential cost. As with all recruits, potential cyber warriors will be questioned regarding previous immoral and illegal activities and be selected or disqualified according to current standards. Through studying hackers, the Air Force can find the motivations and aptitudes of hackers and recruit for those characteristics. The Air Force does not have to recruit individuals who have been convicted of committing any type of crimes, computer or otherwise.

5.2 Recommendations for Further Research

Throughout the research process, many different aspects appeared that were either not within the scope of this thesis but obviously useful for this topic or would require different methodologies or additional time than what was available. Because of these constraints and some of the limitations addressed in Chapter I, it is evident that this work is not the definitive piece on cyberspace warrior selection. Therefore, this section is reserved for topics that are closely related but deemed beyond the scope of this particular research effort. These suggestions range from ways to further explore the topic as it is presented here to suggestions for research on related subjects. Any research into the suggested topics will add to the body of knowledge and facilitate the Air Force efforts to recruit, train, educate, and retain the best individuals as cyberspace warriors.

The first obvious additional research would be studies to determine what levels of motivation and skill are optimal or if it is more important to select individuals with the right aptitudes or with the highest motivation. This research will be difficult until the

aptitude for cyber warriors is truly identified through experiments, exercises, and experience.

The interviews and stories by and about computer hackers were very enlightening. They provided some potential areas of study that could be very useful to a cyberspace force. One of these topics is social engineering. "The social engineer, or the attacker skilled in the art of deception as one of the weapons in his or her toolkit, preys on the best qualities of human nature: our natural tendencies to be helpful, polite, supportive, a team player, and the desire to get the job done" (Mitnick & Simon, 2005). Social engineering is a very effective tool. Not only does the military need to defend against social engineering, but it should be recognized as an offensive tool. Using social engineering against the enemy can provide many advantages the technical computer hack does not offer. In order to complete a social engineering attack, there are many aspects that would need to be considered including language and culture. To successfully pull off a social engineering attack in another country, the attacker would have to be well versed not only in that country's language, but also in the small nuances of the languages, the jargon that might apply to the situation and the cultural customs, courtesies, and mores. As Sun Tzu said, "To know your Enemy, you must become your Enemy" (Wikipedia, 2007).

Further studies regarding gender issues may be useful. The literature suggests that males are more commonly associated with computers than females. In a personal conversation, a senior researcher at the Air Force Research Laboratory stated his belief that females would likely make better network defenders because of their ability to multitask. Other personal conversations have supported the idea that females may be better at defending but offered that it might be because females have an innate desire to

protect what is theirs. It is interesting that there are so few female computer professionals and yet they may have the intuitive motivations or skills to help the computer community. First, research is necessary to determine if the hypothesis that females are better than men at defending a network are true. If this hypothesis is true, further research regarding why they are better is necessary so those traits can be identified and used for recruiting and training the best network defenders as possible.

Although motivation and aptitude are the only factors considered in this thesis, they are not the only factors that determine how good a cyberspace warrior will be. There are many aspects that will contribute to success. As the cyberspace force develops and their roles are formally determined, research for other aspects that predict success will be necessary.

One concern noted during this research was the lack of references to certain subjects that warrant research as they relate to cyber operations. One such subject is steganography, the process of hiding messages within pictures or other forms of communications. Certainly this is an area that could be exploited in cyber warfare. Another subject with little reference was regarding linguistic challenges. If cyber warriors can hack into an adversary's system, a language barrier could cause considerable challenges to remaining undetectable and gathering information. One of the skills cyber warriors may need is a second language.

One final recommended area of study is academic tracks or majors. A college major might indicate self-selection into this type of work, which would indicate the individual probably has the motivation to perform this type of work. Completion of such a college major also indicates some experiences that are important for cyberspace

warriors. Identify classes, technical and non-technical, that would be useful in cyber operations would benefit the filtering process.

5.3 Conclusions

This research has highlighted many challenges of creating a new mission and identifying the correct individuals for that mission. Initially, the task appeared to be straightforward but it quickly grew more complex as more information came available. As the information regarding the cyber force becomes available, research should continue to enhance not only the selection process for cyberspace warriors, but to enhance the cyberspace mission.

One goal of this thesis was to stimulate dialogue regarding the selection of cyberspace candidates and identify the associated problems. Once the challenges are identified, they can be addressed. The second and more formidable goal of this research was to lay a foundation upon which to devise a test or selection method for selecting cyberspace warriors. Without having any previous research in this particular area, results from similar areas were considered. Based on the success of current selection methods when coupled with hacker characteristics, a foundation for selecting cyberspace warriors was formed. Although there are some issues regarding the use of analyzing activities performed illegally by civilians to form a screening method for potential military members, it does provide insight into the skills and motivations needed for a screening process. It also provides insight from a defensive standpoint of protecting networks. Both views are important to the military mission. The military must be prepared to

expend resources on recruiting the *right* people for this mission. These resources will include research time and money, development of the best screening methods, flexibility in adjusting current tests and flexibility to try new screening methods. As the cyberspace mission is now part of the Air Force mission, the Air Force must not waste time in selecting and training candidates. The first of the cyber warriors will be those who contribute not only to defining the mission, but also to creating the tactics, techniques, and procedures future cyber warriors will use. They will have a large impact on the development of the career field and the success of the mission. As the cyber mission is codified, doctrine must be updated and cyber must become an inherent part of all training so it is ingrained in all airmen. This is a worthwhile mission but the Air Force must be careful and disciplined to do it right.

This research offered many thought on the cyberspace mission. Some of the topics are directly related to selection methods while others are not. All ideas were generated by the research conducted for this topic. As cyberspace is a new mission, there are many unknowns and therefore many ideas that must be considered as the mission is formed. The research also resulted in the realization that there are many related topics to research. Research completed in the suggested areas will only enhance the selection process, which, in turn, will enhance the people in the mission and the mission itself. Finally, this research is intended not only to suggest ways to select future cyberspace warriors but to trigger other thoughts, research, and studies on the best ways to do the selection process. As the starting point, it is expected that this work be criticized, but more importantly, it is intended to be used as a way to ignite the discussions and research necessary to select the best cyberspace warriors the U.S. Air Force can.

Appendix A: Glossary of Terms and Abbreviations

AFA – Air Force Academy

AFOQT - Air Force Officer Qualifying Test

AFQT – Armed Forces Qualification Test

AFSC – Air Force Specialty Code

ASVAB – Armed Services Vocational Aptitude Battery

BAT - Basic Attributes Test

CIA – Central Intelligence Agency

CEP – Career Exploration Program

CNA – Computer network attack

CNE – Computer network exploitation

CSAF - Chief of Staff of the Air Force

DoD - Department of Defense

EBM – Evidence based medicine

ECAT - Enhanced Computer-Administered Test

HSGPA – High school grades

IOS – Information Operations Squadron

NSA – National Security Agency

NT – Newbie/tool kit

OTS – Officer Training School

PCSM - Pilot Candidate Selection Method

ROTC – Reserve Officer Training Corps

RSS – Relative Standing Score

SAT - Scholastic Aptitude Test

SAT V + M – SAT verbal and math

SECAF - Secretary of the Air Force

Appendix B: Proposed Blueprint

Panel 1		Panel 2					
Test blueprint		Table of specification levels					
Content area*	% of items on test **	Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
1.0 Software/Application Knowledge							
1.1 Worms							
1.2 Viruses							
1.3 OS vulnerabilities							
1.3.1 Microsoft							
1.3.2 Macintosh							
1.3.3 Linux							
1.4 Other vulnerabilities							
1.4.1 Internet Explorer							
1.4.2 Website vulnerabilities							
1.4.3 E-mail vulnerabilities							
2.0 Programming							
2.1 Basic							
2.2 Unix							
2.3 C++							
2.4 Other languages							
3.0 Network Security							
3.1 Firewall./router rules							
3.2 Passwords							
3.3 Authentication							
3.4 Honey pots							
3.5 Intrusion detection							
4.0 Network Architecture							
4.1 Topology							
4.2 Reference models							
4.3 Common configurations							
4.4 Mapping							
5.0 Ports/protocols							
6.0 Cryptography							
6.1 Symmetric/asymmetric encryption							
6.2 Public key infrastructure							

Figure 7. Proposed Skills Test Blueprint

7.0 Problem Solving							
7.2 Logic problems							
7.3 Mental maps							
7.4 Identifying relationships							
8.0 Social Engineering							
9.0 Hardware							
10.0 Other							

Figure 8. Proposed Skills Test Blueprint (cont.)

Panel 1 consists of all content areas identified for a test.
A test can be broad or specific depending on its purpose

Panel 2 identifies how difficult the questions should be.
The cognitive levels can also be adjusted depending on the purpose and level of the test.

Appendix C: Content Analysis Results

Table 3. Content Analysis Results

Article	Knowledge		gain		power		moral	
	R1	R2	R1	R2	R1	R2	R1	R2
Hackers and the Contested Ontology of Cyberspace (Nissenbaum, 2004)	0	0	0	0	0	0	3	3
Ethical Hacking (Palmer, 2001)	1	0	1	1	1	1	0	0
How to Become a Hacker (Raymond, 2006)	2	1	0	0	1	1	2	2
A New Hacker Taxonomy (M. Rogers, 2003a)	4	4	3	3	3	4	2	3
Information warfare cyber-terrorism cyber criminals (M. Rogers, 2000)	0	0	1	1	0	1	0	0
Theories of Crime and Hacking (M. Rogers, 2003)	1	1	0	0	2	1	1	0
Hackers' Accounts (Turgeman-Goldschmidt, 2005)	4	5	2	1	3	3	1	0
Technical and Human Issues Computer-Based System Security (Arief & Besnard, 2003)	4	1	1	2	4	1	2	1
Profiling Cybercriminals (Bednarz, 2004)	3	1	6	6	2	1	0	0
A Conceptual Model of Hacker Development and Motivations (Beveren, 2001)	4	2	0	1	4	2	0	0
Concerning Hackers who Break into Computer Systems (Denning, 1990)	5	4	0	0	1	1	4	3
A Sociology of Hackers (Jordan & Taylor, 1998)	2	3	0	0	1	2	2	2
Cyberwarriors (Denning, 2001)	1	0	1	1	0	0	3	5
Computer Hackers: Rebels With a Cause (Rosteck, 1994)	5	2	1	1	1	0	3	3
Modeling Behavior of the Cyber-Terrorist (Schudel, Wood, & Parks, 1999)	0	0	1	0	0	0	0	0
International Computer Crimes (Zakaras, 2001)	1	1	0	0	1	0	1	1
An Initial Foray into Understanding Adversary Planning and Courses of Action (Lowry, 2001)	1	0	0	0	0	0	0	0
Organized Computer Crime and More Sophisticated (M. Rogers, 2003b)	0	0	1	1	0	0	0	0
Beyond Conventional Terrorism…The Cyber Assault (Puran, 2003)	0	0	0	0	0	0	5	3
Cognitive Hacking: A Battle for the Mind (Cybenko, Giani, & Thompson, 2002)	0	0	3	2	1	1	0	0
The Role of Criminal Profiling in the Computer Forensics Process (M. Rogers, 2003/5)	0	0	2	1	2	1	1	0
Totals	**38**	**25**	**23**	**21**	**27**	**20**	**30**	**26**

Table 3. Motivation Content Analysis Results (Cont)

Article	obsession		fun		community		other	
	R1	R2	R1	R2	R1	R2	R1	R2
Hackers and the Contested Ontology of Cyberspace (Nissenbaum, 2004)	0	0	0	0	1	1	0	0
Ethical Hacking (Palmer, 2001)	0	0	1	1	0	0	1	2
How to Become a Hacker (Raymond, 2006)	0	0	1	1	0	0	0	0
A New Hacker Taxonomy (M. Rogers, 2003a)	1	1	4	4	1	1	4	6
Information warfare cyber-terrorism cyber criminals (M. Rogers, 2000)	0	0	0	0	1	0	1	2
Theories of Crime and Hacking (M. Rogers, 2003)	0	1	0	1	1	2	0	0
Hackers' Accounts (Turgeman-Goldschmidt, 2005)	0	0	3	5	2	0	5	4
Technical and Human Issues Computer-Based System Security (Arief & Besnard, 2003)	2	1	3	3	1	1	1	2
Profiling Cybercriminals (Bednarz, 2004)	0	0	0	1	1	0	4	1
A Conceptual Model of Hacker Development and Motivations (Beveren, 2001)	1	1	2	1	5	2	2	0
Concerning Hackers who Break into Computer Systems (Denning, 1990)	0	0	3	3	1	0	0	3
A Sociology of Hackers (Jordan & Taylor, 1998)	1	1	1	1	3	1	1	1
Cyberwarriors (Denning, 2001)	0	0	1	1	0	0	2	2
Computer Hackers: Rebels With a Cause (Rosteck, 1994)	0	0	1	0	3	0	0	0
Modeling Behavior of the Cyber-Terrorist (Schudel et al., 1999)	0	0	0	0	0	0	1	0
International Computer Crimes (Zakaras, 2001)	1	0	2	1	0	0	0	0
An Initial Foray into Understanding Adversary Planning and Courses of Action (Lowry, 2001)	0	0	0	0	1	0	0	0
Organized Computer Crime and More Sophisticated (M. Rogers, 2003b)	0	0	0	0	0	0	0	0
Beyond Conventional Terrorism…The Cyber Assault (Puran, 2003)	0	0	0	0	0	0	0	0
Cognitive Hacking: A Battle for the Mind (Cybenko et al., 2002)	0	0	1	0	0	0	1	0
The Role of Criminal Profiling in the Computer Forensics Process (M. Rogers, 2003/5)	0	0	0	0	1	0	4	2
Totals	**6**	**5**	**23**	**23**	**22**	**8**	**27**	**25**

Table 4. Skills Content Analysis Results

Article	Programming		net knowledge		problem		social eng	
	R1	R2	R1	R2	R1	R2	R1	R2
Hackers and the Contested Ontology of Cyberspace (Nissenbaum, 2004)	2	2	0	2	0	0	0	0
Ethical Hacking (Palmer, 2001)	1	1	1	1	0	0	0	1
How to Become a Hacker (Raymond, 2006)	4	3	1	1	3	2	0	0
A New Hacker Taxonomy (M. Rogers, 2003a)	2	2	1	1	0	0	0	0
Information warfare cyber-terrorism cyber criminals (M. Rogers, 2000)	1	1	2	1	1	1	0	0
Theories of Crime and Hacking (M. Rogers, 2003)	0	0	1	1	2	1	0	0
Hackers' Accounts (Turgeman-Goldschmidt, 2005)	1	1	1	1	0	0	0	0
Technical and Human Issues Computer-Based System Security (Arief & Besnard, 2003)	1	1	0	1	0	0	1	1
Profiling Cybercriminals (Bednarz, 2004)	0	0	0	1	0	0	0	0
A Conceptual Model of Hacker Development and Motivations (Beveren, 2001)	1	1	2	0	2	0	1	0
Concerning Hackers who Break into Computer Systems (Denning, 1990)	1	3	2	2	0	0	0	0
A Sociology of Hackers (Jordan & Taylor, 1998)	0	0	0	1	0	0	0	1
Cyberwarriors (Denning, 2001)	0	0	0	2	0	0	0	0
Computer Hackers: Rebels With a Cause (Rosteck, 1994)	0	0	0	0	1	0	0	0
Modeling Behavior of the Cyber-Terrorist (Schudel et al., 1999)	0	0	1	1	0	0	0	0
International Computer Crimes (Zakaras, 2001)	1	1	1	1	0	0	0	0
An Initial Foray into Understanding Adversary Planning and Courses of Action (Lowry, 2001)	0	0	0	0	0	0	0	0
Organized Computer Crime and More Sophisticated (M. Rogers, 2003b)	0	0	0	1	0	0	0	0
Beyond Conventional Terrorism…The Cyber Assault (Puran, 2003)	1	0	2	2	0	0	0	0
Cognitive Hacking: A Battle for the Mind (Cybenko et al., 2002)	0	0	0	1	0	0	0	0
The Role of Criminal Profiling in the Computer Forensics Process (M. Rogers, 2003/5)	0	0	0	0	0	0	0	0
Totals	**16**	**16**	**15**	**21**	**9**	**4**	**2**	**3**

Table 4. Skills content Analysis Results (Cont)

Article	soft/app knowledge		other		hardware		crypto	
	R1	R2	R1	R2	R1	R2	R1	R2
Hackers and the Contested Ontology of Cyberspace (Nissenbaum, 2004)	1	1	0	0	0	1	0	0
Ethical Hacking (Palmer, 2001)	0	1	0	1	0	1	0	0
How to Become a Hacker (Raymond, 2006)	0	1	1	0	0	0	0	0
A New Hacker Taxonomy (M. Rogers, 2003a)	2	1	0	0	1	0	0	0
Information warfare cyber-terrorism cyber criminals (M. Rogers, 2000)	0	0	0	0	1	1	0	0
Theories of Crime and Hacking (M. Rogers, 2003)	0	0	0	0	0	0	0	0
Hackers' Accounts (Turgeman-Goldschmidt, 2005)	0	2	0	0	1	0	0	0
Technical and Human Issues Computer-Based System Security (Arief & Besnard, 2003)	1	3	0	2	1	1	2	1
Profiling Cybercriminals (Bednarz, 2004)	0	1	0	0	0	0	0	0
A Conceptual Model of Hacker Development and Motivations (Beveren, 2001)	0	0	0	0	0	0	1	0
Concerning Hackers who Break into Computer Systems (Denning, 1990)	1	1	0	0	0	0	2	2
A Sociology of Hackers (Jordan & Taylor, 1998)	0	1	0	1	0	0	0	0
Cyberwarriors (Denning, 2001)	0	2	0	0	0	0	1	0
Computer Hackers: Rebels With a Cause (Rosteck, 1994)	0	0	0	0	0	0	0	0
Modeling Behavior of the Cyber-Terrorist (Schudel et al., 1999)	0	0	0	2	0	0	0	0
International Computer Crimes (Zakaras, 2001)	1	1	0	0	0	0	2	1
An Initial Foray into Understanding Adversary Planning and Courses of Action (Lowry, 2001)	0	0	0	0	0	0	0	0
Organized Computer Crime and More Sophisticated (M. Rogers, 2003b)	0	1	0	0	0	0	0	1
Beyond Conventional Terrorism…The Cyber Assault (Puran, 2003)	1	1	0	0	0	0	0	0
Cognitive Hacking: A Battle for the Mind (Cybenko et al., 2002)	0	1	0	0	0	0	0	0
The Role of Criminal Profiling in the Computer Forensics Process (M. Rogers, 2003/5)	0	0	0	0	0	0	0	0
Totals	**7**	**18**	**1**	**6**	**4**	**4**	**8**	**5**

References

Adams, J. (2001). The weakness of a superpower. *Foreign Affairs, 80*(3), 89-97.

AF/A8. (2006). *Air force strategic plan 2006-2008.* Washington D.C.: Department of the Air Force.

aptitude. (n.d.). *The American Heritage® Dictionary of the English Language, Fourth Edition.* Retrieved February 09, 2007, from Dictionary.com website: http://dictionary.reference.com/browse/aptitude

Arief, B., & Besnard, D. (2003). *Technical and human issues in computer-based systems security* (Technical Report No. CS-TR-790). University of Newcastle upon Tyne, UK: School of Computing Science.

Bednarz, A. (2004). *Profiling cybercriminals: A promising but immature science.* Retrieved 11/16, 2006, from http://www.networkworld.com/supp/2004/cybercrime/112904profile.html

Beveren, J. V. (2001). A conceptual model of hacker development and motivations. *Journal of E-Business, 1*(2), Dec 12, 2006 from http://www.dvara.net/HK/beveren.pdf

Bridge, P. D., Musial, J., Frank, R., Roe, T., & Sawilowsky, S. (2003). Measurement practices: Methods for developing content-valid student examinations. *Medical Teacher, 25*(4), 414-421.

Burton, N. W., & Ramist, L. (2001). *Predicting success in college: SAT studies of classes graduating since 1980* No. 2001-2). New York: College Entrance Examination Board.

Busch, C., et al. (2005). *Content analysis. Writing@CSU.* Retrieved Jan 15, 2007, from http://writing.colostate.edu/guides/research/content/index.cfm

Bush, G. W. (2003). *The national strategy to secure cyberspace*. Washington D.C.: The White House.

Camara, W. J., & Echternacht, G. (2000). *The SAT 1 and high school grades: Utility in predicting success in college* No. College Board Report No. RN-10. New York: College Entrance Examination Board.

Carretta, T. (2000). U.S. air force pilot selection and training methods. *Aviation, Space and Environmental Medicine, 71*(9), 950-962.

Clark, D. (2001). *Learning domains or bloom's taxonomy.* Retrieved Jan 29, 2007, from http://www.nwlink.com/~donclark/hrd/bloom.html

Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications. (1989). National security emergency preparedness initiatives to date. *Growing vulnerability of the public switched networks: Implications for national security emergency preparedness* (pp. 1-21). Washington, D.C.: National Academy Press.

Cybenko, G., Giani, A., & Thompson, P. (2002). Cognitive hacking: A battle for the mind. *IEEE Computer Society, 35*(8), 50-56.

Cyber Forces Education and Training Workshop. (2007). *Cyber forces education and training potential end states and courses of action (draft).* Unpublished manuscript.

Denning, D. E. (2001). Cyberwarriors activists and terrorist turn to cyberspace. *Harvard International Review, XXIII*(2), 70-75.

Denning, D. E. (1990). Concerning hackers who break into computer systems. *13th National Computer Security Conference,* Washington D. C. from http://www.sgrm.com/art-7.htm

Department of the Air Force. (2003). *Air force basic doctrine (AFDD) 1*. Washington D.C.: Department of the Air Force.

Downing, S. M., & Haladyna, T. M. (1997). Test item development: Validity evidence from quality assurance procedures. *Applied Measurement in Education, 10*(1), 61-82.

Ebel, R. L. (1972). *Essentials of educational measurement* (2nd ed.). Englewood Cliffs, New Jersey: Prentice Hall, Inc.

Gatewood, R. D., & Feild, H. S. (2001). *Human resource selection* (5th ed.). Orlando, FL: Harcourt, Inc.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI computer crime and security survey*Computer Security Institute.

hacker. (n.d.). *The American Heritage® Dictionary of the English Language, Fourth Edition.* Retrieved February 09, 2007, from Dictionary.com website: http://dictionary.reference.com/browse/hacker

Hallion, R. P. (1987). Doctrine, technology, and air warfare. *Airpower Journal, Fall*(4), 61-80.

Herrington, A. (2004). *Maslow's hierarchy, societal change and the knowledge worker revolution.* Retrieved Jan 24, 2007, from http://www.pateo.com/article6.html

Himanen, P. (2001). *The hacker ethic and the spirit of the information age*. New York, NY: Random House Inc.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological review, 46*(4), 757-780.

Kakabadse, N. K., Kouzmin, A. & Chatham, R. (2002). *IS/IT professionals' personality difference: A case of selection or predisposition?* Retrieved 12/01, 2006, from http://www.scu.edu.au/schools/socialsciences/ajbsi/papers/vol2/is_it_prof.pdf

Kobrin, J. L., & Michel, R. (2006). *The SAT as a predictor of different levels of college performance*. New York: The College Board.

Kass, L. (2006). *A warfighting domain* Air Force Cyberspace Task Force.

Laurance, J. H. (2004). *Performance of the all-volunteer force*. Washington, D.C.: Office of the Under Secretary of Defense (Force Management Policy). Retrieved 20 Nov 2006, from http://www.rand.org/pubs/monographs/MG265/images/webS0838.pdf

Libicki, M., & Shapiro, J. (1999). Conclusion: The changing role of information in warfare. In Z. Khalilzad, J. P. White & A. W. Marshall (Eds.), *Strategic appraisal: The changing role of information in warfare* (pp. 437-452). Santa Monica, CA: Rand.

Lowe, P. J. (1998). Zero-based language aptitude test design where's the focus for the test? *Applied Language Learning, 9*(1 & 2), 11-30.

Lowry, J. (2001). An initial foray into understanding adversary planning and courses of action. *DARPA Information Survivability Conference and Exposition,* from http://ieeexplore.ieee.org/iel5/7418/20170/00932201.pdf?tp=&arnumber=932201&isnumber=20170

Mayer, D. B., & Stalnaker, A. W. (1968). Selection and evaluation of computer personnel- the research history of SIG/CPR. *ACM/CSC-ER Proceedings of the 1968 23rd ACM National Conference* , 657-670.

Miller, L. T. (1999). Psychometric and information processing approaches to measuring cognitive abilities: Paradigms in military testing. *Canadian Psychology,*

Mitnick, K. D., & Simon, W. L. (2005). *The art of intrusion the real sories behind the exploits of hackers, intruders & deceivers*. Indianapolis, IN: Wiley Publishing, Inc.

motivation. (n.d.). WordNet® 2.1. Retrieved February 09, 2007, from Dictionary.com website: http://dictionary.reference.com/browse/motivation

Nelson, R. R., & Todd, P. A. (2004). Peopleware: The hiring and retention of IT personnel. *Strategies for managing IS/IT personnel* (pp. 1-17). Hershey, PA: Idea Group Publishing.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society, 6*(2), 195-217.

Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal, 40*(3), 769-780.

Parks, R. C., & duggan, D. P. (2001). Principles of cyber-warfare. *Proceeding of the 2001 IEEE Workshop on Information Assurance and Security,* United States Military Acadamy, West Point, NY. 122-125.

Puran, R. C. (2003). *Beyond conventional terrorism... the cyber assault,* SANS Institute.

Rathmell, A. D. (1997). Cyberterrorism: The shape of future conflict? *Royal United Service Institute Journal,* 40-46.

Raymond, E. S. (2006). *How to become A hacker.* Retrieved December 29, 2006, from http://catb.org/esr/faqs/hacker-howto.html

Robinson, D. J. (2007). *315 IOS mission orientation briefing* (Wright Patterson Air Force Base ed.)

Rogers, M. (2003). *A new hacker taxonomy.* Retrieved November, 2006, from homes.cerias.purdue.edu/~mkr/hacker.doc

Rogers, M. (2003). *Organized computer crime and more sophisticated security controls: Which came first the chicken or the egg?* Retrieved 11/28, 2006, from http://64.233.167.104/search?q=cache:TmPF78kFbTEJ:homes.cerias.purdue.edu/~mkr/Org.doc+organized+computer+crime+and+more+sophisticated+security+controls&hl=en&ct=clnk&cd=1&gl=us

Rogers, M. (2000). *Information warfare cyber-terrorism cyber-criminals.* Retrieved Dec 12, 2006, from http://homes.cerias.purdue.edu/~mkr/

Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers & Security, 22*(4), 292-298.

Rogers, M. (2003). Psychological theories of crime and hacking. (M.A. CISSP, University of Manitoba). 1-26.

Rosteck, T. S. (1994). *Computer hackers: Rebels with a cause.* Concordia University.

Schneier, B. (2000). *Secrets and lies digital security in a networked world*John Wiley & Sons, Inc.

Schudel, G., Wood, B., & Parks, R. (1999). Modeling behavior of the cyber-terrorist. *National Security Forum on International Cooperation to Combat Cyber Crime and Terrorism,* Hoover Institution, Stanford University.

Sellman, W. S. (2004). *Predicting readiness for military service how enlistment standards are established* (Prepared for the National Assessment Governing Board)

Turgeman-Goldschmidt, O. (2005). Hackers' accounts hacking as a social entertainment. *Social Science Computer Review, 23*(1), 8-23.

Welsh, John R. Jr., Kucinkas, S. K., & Curran, L. T. (1990). *Armed services vocational battery (ASVAB): Integrative view of validity studies* No. AFHRL-TR-90-22). Brooks AFB, TX: Air Force Human Resources Laboratory.

Wikipedia. (2007). *Sun tzu.* Retrieved Feb 22, 2007, from http://en.wikiquote.org/wiki/Sun_Tzu

Wynne, M. W. (2006). In C4ISR Integration Conference, Crystal City, VA (Ed.), *Cyberspace as a domain in which the air force flies and fights*

Wynne, M. W., & Moseley, T. M. (2005). *SECAF/CSAF letter to airmen: Mission statement*

Young, J. W., & Kobrin, J. L. (2001). *Differential validity, differential prediction, and college admission testing: A comprehensive review and analysis* No. College Board Research Report No. 2001-6. New York: College Entrance Examination Board.

Zakaras, M. R. (2001). International computer crimes. *Revue Internationale de Droit Pénal, 72*(3-4), 813-829.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
22-03-2007	MS Thesis	Jan 2006 - March 2007

4. TITLE AND SUBTITLE

In Pursuit of an Aptitude Test for Potential Cyberspace Warriors

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Tiffiny S. Smith

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management Building 640
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENG/07-01

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

Maj David Robinson 315 IOS
9800 Savage Road
Suite 6530
Ft Meade, MD 20755
email: david.robinson3@lackland.af.mil phone: (240) 373-2338

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 Air Force has officially assumed the cyberspace mission. In order to perform the mission to the best extent possible, it is important to employ personnel with the necessary skill sets and motivation to work in this type of environment. The first step in employing the right people is to screen all possible candidates and select those with an aptitude for acquiring the skill sets and the motivation to perform this work. This thesis is an attempt to determine the necessary skills and motivations to perform this work and recommend a screening process to select the candidates with the highest probability for success. Since this mission is new, determining what skills and motivations are necessary is difficult. To assist in determining the skills and motivations for cyber warriors, this thesis considers the skills and motivations of computer hackers. If the skills and motivations of successful hackers can be identified, those skills and motivations can be used as a tool for developing an aptitude test to be used as a screening device. A blueprint for an aptitude test is provided based on the findings of the hacker skills and motivations.

15. SUBJECT TERMS

Cyberspace, cyberspace warriors, aptitude tests, skills, motivations, computer hackers

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Robert F. Mills rober.mills@afit.edu
U	U	U	UU	103	19b. TELEPHONE NUMBER *(Include area code)* (937) 785-3636 x 4527