



**EVALUATING THE EFFECTIVENESS OF AIR FORCE  
FOUNDATIONAL CYBERSPACE TRAINING**

GRADUATE RESEARCH PROJECT

April L. Wimmer, Major, USAF

AFIT/ICW/ENG/12-05

**DEPARTMENT OF THE AIR FORCE  
AIR UNIVERSITY**

**AIR FORCE INSTITUTE OF TECHNOLOGY**

---

---

**Wright-Patterson Air Force Base, Ohio**

DISTRIBUTION STATEMENT A.  
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this report are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT/ICW/ENG/12-05

EVALUATING THE EFFECTIVENESS OF AIR FORCE  
FOUNDATIONAL CYBERSPACE TRAINING

GRADUATE RESEARCH PROJECT

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 Cyber Warfare

April L. Wimmer, MS

Major, USAF

June 2012


DISTRIBUTION STATEMENT A.  
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

**EVALUATING THE EFFECTIVENESS OF AIR FORCE  
FOUNDATIONAL CYBERSPACE TRAINING**

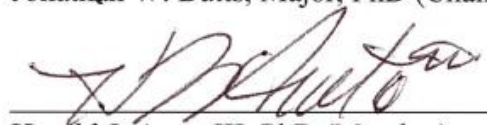
April L. Wimmer

Major, USAF

Approved:

  
Jonathan W. Butts, Major, PhD (Chairman)

29 May 2012  
Date

  
Harold J. Arata III, PhD (Member)

29 MAY 2012  
Date

### **Abstract**

Cyberspace is pervasive in military operations across all domains and is vital to how the United States conducts those operations. The Air Force recognized the importance of cyberspace to the successful completion of its missions and designated it a domain equal with Air and Space. Additionally, the Air Force understood that each Airman's actions and activities on the network affected every other Airman and impacted the ability to execute the broader Air Force mission. Therefore, they introduced the "Cyber Wingman Philosophy" to guide Airmen's daily cyberspace conduct. In addition, they instituted cyberspace training at Basic Military Training and Officer Accession programs.

This paper examines the effectiveness of cyberspace training established for all Active Duty Air Force officer and enlisted members. Specifically, it summarizes current training, reviews the mechanisms established to evaluate the effectiveness of that training, and determines if current training programs are meeting the desired Air Force training goals. The research uses a twofold approach. First, it applies inductive research to analyze the existing training and evaluation mechanisms. Second, it includes a survey mechanism to evaluate the attitudes of individuals who have received the "Cyberspace and the Air Force" training.

The research concludes that the next step in Air Force cyberspace training is to determine the effectiveness of the training. Analysis revealed the need to establish clearly defined objectives for Air Force Foundational Cyberspace Training; complete pre

and post training attitude assessment surveys; and inclusion of curriculum developers in the feedback process. It is not sufficient to implement training and declare victory. Cyberspace is critical to successful operations and the Air Force must ensure the quality of the training mirrors the importance of the mission.

*To Amelia, Steven, and my family  
Your endless love and support make it all possible!*

## **Acknowledgments**

I would like to express my sincere appreciation to the entire staff at the Air Force Institute of Technology Center for Cyberspace Research. Your professionalism and support is greatly appreciated. I would like to offer a special thank you to Senior Master Sergeant Wabiszewski for the expertise and the invaluable assistance he provided during this research.

I am grateful to my research advisor, Major Jonathan Butts, for his guidance and support throughout the course of this effort. You provided the focus and direction to keep the project on track.

I would also like to thank Dr. Harold Arata for his support over the past year. His enthusiasm is contagious and his passion for both cyberspace and the Air Force provided continual motivation.



## Table of Contents

	Page
Abstract .....	iv
Acknowledgments.....	vii
Table of Contents .....	viii
List of Figures .....	x
List of Tables .....	xi
List of Abbreviations .....	xii
I. Introduction .....	1
1.1 Cyber Added to Air Force Mission Statement .....	1
1.2 Rise of the Cyber Wingman .....	2
1.3 Need for Training .....	2
1.4 Paper Objectives and Scope.....	3
1.5 Organization .....	3
II. Background .....	5
2.1 What is Air Force Foundational Cyber Space Training?.....	5
2.2 Current USAF Cyberspace Training .....	5
2.2.1 Enlisted Training.....	5
2.2.2 Officer Training .....	7
2.3 Mechanisms for Evaluating USAF Cyberspace Training .....	11
2.3.1 Instructional System Development .....	11
2.3.2 Advanced Distributed Learning .....	14
2.4 Establish a Baseline .....	15
2.4.1 What is the Required Knowledge Level .....	15
2.4.2 Average Level of Knowledge Prior to Training .....	16
2.4.3 Average Level of Knowledge Post Training.....	18
2.5 Background Summary .....	19
III. Evaluation of Cyberspace Training .....	20
3.1 Approach.....	20
3.2 Likert Survey .....	21
3.3 Survey Demographics.....	25
3.4 Results of the Likert Survey .....	27
3.5 Evaluation of Cyberspace Training Summary .....	29

IV. Analysis and Recommendations .....	31
4.1 Determine the Objective of the Training .....	31
4.2 Establish the Baseline .....	33
4.3 Involve Curriculum Developers in the Process .....	35
4.4 The Need for Feedback.....	37
4.5 The Illusion of Progress Can Be Dangerous.....	39
4.6 Analysis and Recommendations Summary .....	40
V. Conclusions .....	42
5.1 Impact on the Air Force .....	42
5.2 Limitations of this Work.....	43
5.3 Areas for Future Study.....	43
5.4 Closing Thoughts.....	44
Appendix A - Letter to Airmen 2005.....	46
Appendix B - Rise of the Cyber Wingman.....	47
Appendix C – Likert Survey .....	48
Appendix D – Likert Subcategories.....	51
Appendix E – Likert Summation and Average.....	53
Appendix F – Likert Responses Per Rating.....	55
Bibliography .....	56

## List of Figures

Figure	Page
1. ISD Model.....	12
2. ISD Evaluation Steps .....	13
3. ADDIE Model.....	15
4. Kirkpatrick Four Levels .....	16
5. Sample Exercise Message.....	38

## List of Tables

Table	Page
1. AFSCs Surveyed.....	26

## **List of Abbreviations**

<b>Abbreviation</b>	<b>Acronym</b>
ACE	Advanced Cyberspace Education
ADDIE	Analysis, Design, Development, Implementation, and Evaluation
ADL	Advanced Distributed Learning
ADLS	Advanced Distributed Learning System
AF CyTCoE	AF Cyberspace Technical Center of Excellence
AFLC	Air Force Learning Center
AFOQT	Air Force Officer Qualifying Test
AFSC	Air Force Specialty Code
ASVAB	Armed Forces Vocational Aptitude Battery
BMT	Basic Military Training
MTI	Military Training Instructor
OTS	Officer Training School
PII	Personally Identifiable Information
ROTC	Reserve Officer Training Corps
USAFA	United States Air Force Academy

# **EVALUATING THE EFFECTIVENESS OF AIR FORCE FOUNDATIONAL CYBERSPACE TRAINING**

## **I. Introduction**

### **1.1 Cyber Added to Air Force Mission Statement**

On December 7, 2005, Secretary of the Air Force, Michael Wynne, and Air Force Chief of Staff, General T. Michael Moseley, issued a Letter to Airmen in which they added cyberspace to the Air Force Mission statement (Appendix 1). The Air Force's new mission statement read "The mission of the United States Air Force is 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." Additionally, they recognized cyberspace as a domain equal with Land, Sea, Air, and Space when they stated "Our adversaries will contest us across all of the domains: Land, Sea, Air, Space, and Cyberspace" [1]. These were significant steps because the Air Force was acknowledging the vital importance of cyberspace operations in the conduct of modern warfare.

In May 2007, Secretary Wynne issued another Letter to Airmen in which he stated "our adversaries are attempting to access American servers that contain sensitive data." He went on to state "In response to these threats, Airmen are actively 'flying and fighting' in cyberspace. Our cyber Airmen's work is a prerequisite to all military operations: ensuring freedom of action across the electromagnetic spectrum, which in turn contributes to freedom from attack and freedom to attack in all other domains: land, sea, air and space" [2]. As the advantages gained through cyberspace were increasing, so were the threats from adversaries.

## **1.2 Rise of the Cyber Wingman**

While not every Airman in the Air Force flies a plane, every Airman in the Air Force is involved in cyberspace activities. Sensing the growing threat and vulnerabilities associated with operating in cyberspace, the Air Force decided that it was essential to provide some level of cyberspace training to all Airmen, not just those assigned to cyberspace related specialty codes. In 2009, Air Force Chief of Staff, General Norton Schwartz, outlined the overarching philosophy that incorporates the principles that every Airman should know and use to secure cyberspace (Appendix 2). An Air Force press release announcing the Cyber Wingman philosophy stated “The most common way of getting information is phishing. This attack targets the weakest link in network security: the user.” The article went on to state “phishing happens at work or home” [3].

In addition to recognizing the threats to Air Force networks, the article stated that the defense of the network was the responsibility of everyone on the network. The Commander of Air Force Space Command, General C. Robert Kehler, said “Applying our Wingman culture in the cyberspace domain gives us a powerful advantage – every Airman is a defender in cyberspace.” Air Force Chief of Staff, General Norton Schwartz, echoed this ideology when he said “We must all conduct ourselves as ‘Cyber Wingmen’, recognizing that our actions and activities on the network affect every other Airman and impact our ability to execute the broader Air Force mission” [3].

## **1.3 Need for Training**

With the recognition of the importance of cyberspace and the Rise of the Cyber Wingman Philosophy, came the need to develop training for every Airman. The press

release outlining the Cyber Wingman Philosophy stated “The activation of 24th Air Force August 18th helps define Air Force requirements and establishes training standards for cyber warriors. The next step is to educate every Airman about the Cyber Wingman campaign” [3]. Thus, the Air Force instituted many training initiatives to educate its members and impart the Cyber Wingman philosophy. This paper is dedicated to evaluating the effectiveness of this Air Force Foundational Cyberspace Training.

#### **1.4 Paper Objectives and Scope**

The objective of this paper is to examine the effectiveness of cyberspace training established for all Air Force officer and enlisted members. Specifically, it summarizes current training, reviews the mechanisms established to evaluate the effectiveness of that training, and determines if current training programs are meeting the desired Air Force training goals.

This research is limited to Air Force active duty officer and enlisted personnel. For the purposes of this research, the term cyberspace training includes both cyberspace training and information assurance training. It covers training that members receive during their initial entry into the Air Force (i.e., Basic Military Training, Officer Training School, Reserve Officer Training Corp, and the United States Air Force Academy) and annual reoccurring training for members on active duty (i.e., Advanced Distributed Learning System Information Assurance Awareness and Information Protection courses).

#### **1.5 Organization**

Chapter 2 presents background information necessary to establish the framework for the research conducted, including key definitions, current training, evaluation



mechanisms, and establishing a baseline. Chapter 3 discusses the research approach, methodology used during the development of the survey mechanism, and the survey results. Using the research results, Chapter 4 provides analysis and recommendations. This includes the need to determine training objectives, establish a baseline, involve curriculum developers in the process, provide feedback, and cautions against the illusion of progress. Finally, Chapter 5 concludes by discussing the potential impacts of the research for the Air Force, limitations of the research, and potential areas for future study.

## **II. Background**

### **2.1 What is Air Force Foundational Cyber Space Training?**

Before examining what cyberspace training currently exists in the Air Force, it is necessary to define what constitutes cyberspace training. This research is limited to training that is formally recognized and mandated by the Air Force. More specifically, it focuses on those programs that are intended for all members of the Air Force. Training for cyberspace-specific specialty codes and unit level training is not examined in this research. Air Force Policy Directive 36-26 defines training as a “Set of events or activities presented in a structured or planned manner through one or more media for the attainment and retention of skills, knowledge, and attitudes required to meet job performance requirements” [4]. For this research, Air Force Foundational Cyber Space training includes formally recognized and mandated Air Force cyberspace related training intended for all Active Duty Air Force members.

### **2.2 Current USAF Cyberspace Training**

#### **2.2.1 Enlisted Training**

A review of cyberspace training received by all enlisted members reveals two formal training programs. First, there is the “Cyberspace and the Air Force” training at Basic Military Training (BMT), which was the impetus for conducting this research. Additionally, enlisted members receive annual training via the Advanced Distributed Learning System (ADLS).

In February 2010, the Commander of Air Force Space Command, General C. Robert Kehler, requested that cyberspace training be added to Air Force BMT. The Commander

of Air Education and Training Command, General Stephen R. Lorenz, concurred with the recommendation and a formal task was generated by Headquarters Air Education and Training Command [5]. The Air Force's Cyberspace Technical Center of Excellence (AF CyTCoE) was tasked to develop the curriculum. This was fitting since the AF CyTCoE was chartered to be "a unifying and synergistic body for promoting cyberspace education, training, research, and technology development" [6]. The AF CyTCoE developed material for inclusion in the Airman's study guide, which included a review exercise to assist Airmen as they prepare for the end-of-course exam. They also developed a four hour block of classroom training to be administered by a Military Training Instructor (MTI). This included a flash media presentation and a Plan of Instruction to guide instructors during the presentation of the material. Finally, they developed questions for inclusion in the end-of-course written test that is administered during the seventh week of training and is designed to measure the trainees' comprehension of the academic material presented during BMT [5]. The first BMT trainees to receive the training graduated in October 2010.

Once members complete BMT they are required to accomplish annual ancillary training. Ancillary training is defined as universal training, guidance or instruction, regardless of Air Force Specialty Code (AFSC), that contributes to mission accomplishment [7]. All Air Force military and civilian employees, to include non-appropriated fund and contractor personnel are required to complete Information Protection and Information Assurance Awareness modules of training. This training is described as "general awareness-level training." Information Protection training is designed "to ensure security and protection of DoD information" and Information

Assurance Awareness “ensures personnel are aware of latest threats to computer security issues and how to protect against them” [7]. Airmen receive this training by completing two modules of training via Advanced Distributed Learning (ADL) methods. For the Air Force, the ADLS delivers ADL content and tracks student progress [7].

### **2.2.2 Officer Training**

Officers receive their commission via three distinct sources: United States Air Force Academy (USAFA), Officer Training School (OTS), and Reserve Officer Training Corps (ROTC). Each of the commissioning sources implements a different form of cyberspace training. This section offers a brief overview of the training presented by each commissioning source. Additionally, officers complete the annual Information Assurance Awareness and Information Protection training via the ADLS.

The Air Force Academy cadet wing consists of approximately 4,604 cadets and USAFA produces roughly one quarter of all new Air Force officers each year [8]. Half of those officers attend pilot training while the others enter a wide variety of Air Force specialties. The USAFA cyber training program was developed in coordination with Air University, the Air Force Institute of Technology and Air Force Cyber Command (provisional) [9]. The Academy offers a two-pronged approach: provide a multi-disciplinary foundation for every graduate and develop a smaller number of highly skilled, very technical, cyber warriors. This research focuses on the first prong of their training. According to USAFA officials, “Regardless of their assigned career field, all graduates of the Air Force Academy must possess the specific knowledge, skills, and abilities in the cyberspace domain to effectively serve as Air Force officers in an information-dominated 21st century” [9]. USAFA training focuses on providing cadets

with the technical foundation to operate in cyberspace and augments the training with ethical, legal studies, behavioral science, and military strategic studies. USAFA “aims to produce officers that can not only effectively operate and fight in cyberspace, but officers that do so in a legal and ethical manner with full understanding of the complexities of the human and military strategy as applied to the domain of cyberspace” [9]. USAFA cyberspace training is also included in the core curriculum. The core curriculum is the mandatory set of courses all cadets must complete regardless of their academic major. Additionally, cyberspace training is included in various military training events such as the Basic Cadet Training. Finally, USAFA offers upperclass cadets the opportunity to spend one of their summer sessions in Cyber 256, Basic Cyber Operations. The course is intended to spark cadets’ interest in pursuing more in-depth work in computer science. According to a USAFA news release “everything about the Basic Cyber course emphasizes practical application” [10].

The second source of commissioning is the ROTC. This includes four regional headquarters, 144 detachments and more than 1,200 cross-town universities [11]. In 2011, ROTC commissioned more than 1,796 second lieutenants who entered active duty [8]. ROTC cadets receive two hours of instruction via lecture and guided discussion on cyberspace. This training occurs during their fourth year (senior) of training and it is designed to prepare them for life in the Air Force. The lesson plan lists the cognitive lesson objectives as “Know basic facts and significant vulnerabilities associated with cyberspace operations and the Air Force role in the cyberspace domain.” It identifies cognitive samples of behavior as:

- Define cyberspace and cyber superiority

- Identify specific threats and vulnerabilities associated with cyberspace operations
- Define the unique relationship of the cyberspace domain to other air and space domains according to the Airman's perspective of cyberspace
- State the roles and responsibilities of all Cyber Wingmen.

In addition, the lesson plan states the affective lesson objective is to “Value the need for every Airman to defend the Cyberspace domain against threats.” The sample of behavior prescribed for the objective is to “Respond during guided discussion to the importance of the cyberspace domain” [12]. According to the lesson plan, students are objectively tested on the cognitive samples. This is accomplished via an end-of-course test. The affective objective and samples of behavior are included to provide indications that the students not only understand, but also value the information presented surrounding the objective. This objective is assessed by student responses that demonstrate the affective samples of behavior, typically in response to how and why questions. Instructors are directed that “Responses that communicate feelings in line with the objective are the first level of determining whether you are reaching the affective learning objective with your students” [12]. Like the BMT lesson, this training covers the tenants of the Cyber Wingman Philosophy.

Furthermore, there is some cyberspace training that is ROTC detachment specific. For instance, AFROTC Detachment 003 at the University of Houston hosted a guest speaker, Commander 318th Information Operations Group, to discuss research opportunities related to cyber warfare and cyber security [13] whereas, the Louisiana Tech ROTC program contains a “Cyberspace and the Air Force Mission” lesson. This specific lesson contains three portions. The first portion is designed to give students an

overview of what cyberspace is and its importance to society and the Air Force mission. The second portion highlights the nature of the threats in cyberspace and the third portion discusses Air Force operations in cyberspace [14].

Perhaps the most prominent cyberspace training programs referenced on the various ROTC Detachment websites is the Advanced Cyberspace Education (ACE). ACE is a summer program for junior and senior ROTC cadets studying computer science, computer engineering and electrical engineering. ACE is the nation's only cyber security program for ROTC cadets that combines cyber warfare education, hands-on training, and research internships with Air Force scientists and engineers [6]. However, this program is only attended by a fraction of ROTC cadets.

OTS Commissioned Officer Training and Basic Officer training produced 1,863 officers in 2011 [8]. OTS graduates enter all Air Force Total Force components to include active duty, Air Force Reserve, and Air National Guard. The number of officers trained each year fluctuates in response to variations between projected and actual USAFA and AFROTC officer accessions [15]. The Basic Officer Training syllabus for academic year 2010-2011 included a lesson titled "Cyberspace." This is the same lesson plan that is presented to ROTC cadets. Additionally, there is a lesson titled "Information Assurance, Computer Security, and Information Operations." The objective for this lesson is "Know the fundamental characteristics of Information Assurance, Computer Security, and Information Operations." The lesson description specifies "The objective of the lesson is for the trainees to know the fundamentals of information awareness and computer security and respond to the importance of protecting information systems. It challenges the trainee to take an active role maintaining computer system security" [16].

## **2.3 Mechanisms for Evaluating USAF Cyberspace Training**

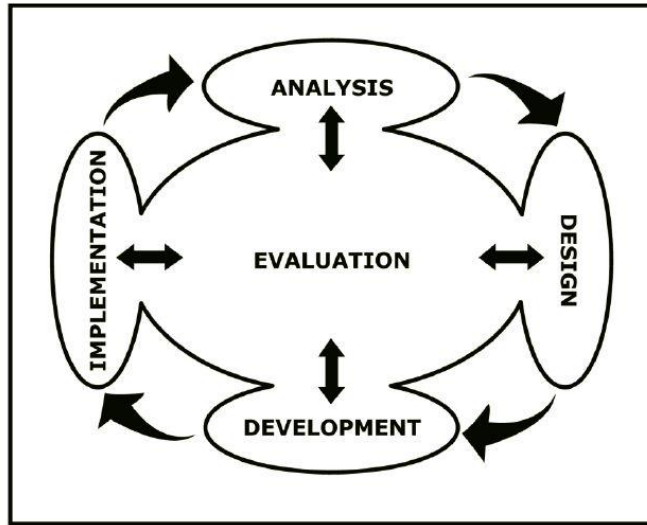
The aforementioned cyberspace training can be summarized according to three categories: enlisted training, officer training, and annual training. This section examines how each of the three training programs currently assesses the effectiveness of their cyberspace training.

In today's fiscally constrained environment it is imperative that every training dollar and man-hour spent achieves the maximum effectiveness. According to Air Force Handbook 36-2235 Volume 1, "Education and training are essential for the effective operation of the Air Force, but can be expensive and can account for a large portion of the Air Force's annual budget." The manual goes on to state "There is a tendency to assume that instruction is the solution for every operation problem. This assumption results in wasted dollars" [17]. Evaluation allows organization to determine their return on investment for training programs.

### **2.3.1 Instructional System Development**

Since 1965, the Air Force has used the Instructional System Development (ISD) process to guide the development of training. ISD is a "systematic, flexible, proven process for determining whether instruction is necessary in a given situation, for defining what instruction is needed, and for ensuring development of effective, cost-efficient instruction" [17]. Figure 1 depicts the phases of the ISD process: analysis, design, development, implementation and evaluation. All phases of the model depend on each of the other phases with evaluation shown as the central feedback network for the total system [18].

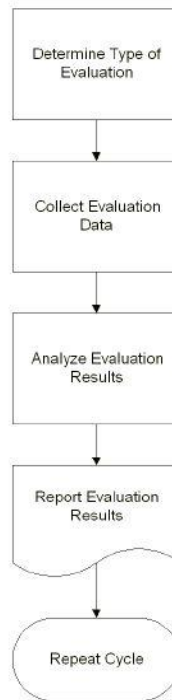




**Figure 1 ISD Model**

Air Force Handbook 36-2235 Volume 13 provides specific information and guidance for applying the ISD process to BMT for enlisted personnel. Figure 2 outlines the five steps of the ISD evaluation phase: determine the type of evaluation, collect evaluation data, analyze evaluation results, report evaluations results, and repeat the cycle.

## Evaluation



**Figure 2 ISD Evaluation Steps**

According to the ISD methodology, once a training program or revisions to a training program are made and the program is implemented and starts producing graduates, it is time to conduct operational evaluations. Operational evaluation is a continuous process that assesses how well course graduates are meeting established job performance requirements [18]. These evaluations may be internal or external evaluations. Some methods for conducting internal evaluations include instructor comments, trainee critiques, and test results. External evaluations are typically accomplished through survey questionnaires and inspection or evaluation reports. The focus of external evaluations is to determine if graduates are meeting established job performance requirements. For “Cyberspace and the Air Force” training, the data collection method is

via a written test. For BMT, “when students successfully achieve the minimum overall passing score on a written test, it implies they have achieved individual objectives and it provides an acceptable degree of confidence that they have attained the required knowledge” [19].

### **2.3.2 Advanced Distributed Learning**

The Department of Defense launched the ADL initiative in November 1997. The intent of ADL is to accelerate large-scale development of dynamic and cost-effective learning environments [20]. As previously mentioned, all Air Force members receive annual Information Protection and Information Assurance Awareness training via ADLS.

Evaluation of ADLS training uses similar methodology to BMT training. According to the ADLS website, the Air Force uses Analysis, Design, Development, Implementation, and Evaluation (ADDIE) process for the development of ADLS curriculum. ADDIE is a colloquial term used to describe a systematic approach to instructional development, virtually synonymous with instructional systems development [21]. Figure 3 depicts the steps of the ADDIE process. Note that similar to ISD, evaluation is at the center of the process.

For ADLS training, evaluation is primarily conducted by test evaluations conducted during the training or an end-of-course test. These tests are administered electronically as part of the training and normally consist of multiple choice or True/False question types. The Information Assurance Awareness training goes further than generalized knowledge-level training and requires trainees to demonstrate concepts associated with the required training. For example, trainees must successfully change a simulated password in order to demonstrate an understanding of establishing strong passwords.



**Figure 3 ADDIE Model**

## **2.4 Establish a Baseline**

### **2.4.1 What is the Required Knowledge Level**

The Kirkpatrick model has served as the primary organizing design for training evaluations in for-profit organizations for over thirty years [22]. The success and wide spread implementation of the Kirkpatrick model make it an ideal methodology for evaluating the status of Air Force cyberspace training. Kirkpatrick outlines four levels: reaction, learning, behavior, and results [23]. Figure 4 shows the four levels of the Kirkpatrick model along with a brief description of each level.

<b>Level 4: Results</b>	To what degree targeted outcomes occur, as a result of the learning event(s) and subsequent reinforcement.
<b>Level 3: Behavior</b>	To what degree participants apply what they learned during training when they are back on the job.
<b>Level 2: Learning</b>	To what degree participants acquire the intended knowledge, skills, and attitudes based on their participation in the learning event.
<b>Level 1: Reaction</b>	To what degree participants react favorably to the learning event.

[23]

**Figure 4 Kirkpatrick Four Levels**

#### **2.4.2 Average Level of Knowledge Prior to Training**

According to Jim and Wendy Kirkpatrick, much of their training and consulting involves helping to negotiate expectations. In a White Paper reviewing the Kirkpatrick model after 50 years of implementation, they stated what normally happens when executives ask for new training is learning professionals jump to the task and commence to design and develop suitable programs. While a cursory need assessment may be

conducted, it is rarely taken to the point that training expectations are completely clear [23].

The previous sections outline the importance of cyberspace operations to the Air Force and demonstrate that individual actions on the network can have far reaching implications. Indeed, all users have an obligation to conduct cyberspace operations in a safe and secure manner. While the requirement is understood, what is not clear is the skill set and knowledge level of Air Force personnel. A need for training indicates that members are not displaying the desired behavior or level of knowledge. All Airmen enlisting in the Air Force take the Armed Forces Vocational Aptitude Battery (ASVAB), which covers four areas: arithmetic reasoning, word knowledge, paragraph comprehension, and mathematics knowledge [24]. Anyone wishing to be an officer in the Air Force must first pass the Air Force Officer Qualifying Test (AFOQT). This test is similar to the Scholastic Aptitude Test and covers topics ranging from verbal and math skills to pilot and navigation aptitude for those interested in those career fields [24]. The test consists of 12 subtests that are used to derive a composite score in five areas: Pilot, Navigator-Technical, Academic Aptitude, Verbal, and Quantitative [25]. Neither the ASVAB nor AFOQT contain mechanisms for evaluating an individual's cyberspace knowledge level.

According to the Air Force Personnel Center, 44% of enlisted Airmen and 13% of officers are below the age of 26 [26]. This statistic does not include cadets at USAFA but USAFA entrance criteria mandates that applicants must not have passed their 23rd birthday by July 1 of the year entering [27]. There is evidence to suggest that this demographic, those between the ages of 18-26, have extensive experience using digital or

cyberspace devices. According to the Pew Internet & American Life Project, 95% of the Millennials (18-34 years old as defined by the Project) own a cell phone and 70% own a laptop computer. When comparing cell phone, desktop and laptop computers, mp3 players, game consoles, e-book readers and tablet usage the project reported that “in terms of generations, Millennials are by far the most likely group to own most of the devices we asked about, but also to take advantage of a wider range of functions” [28]. This fact must be taken into consideration when developing cyberspace training for members of the Air Force. While there is ample evidence to support the assertion that individuals entering the Air Force are already using cyberspace technologies prior to entry, there is not the same type of research to indicate their understanding of how the Air Force uses cyberspace, potential threats to Air Force cyberspace operations, or how their actions could introduce network vulnerabilities. Being technologically savvy does not equate to understanding and implementing cyber security principles.

#### **2.4.3 Average Level of Knowledge Post Training**

The Kirkpatrick model levels are an excellent starting point for assessing the effectiveness of training. First, the Air Force should be able to determine to what degree participants react favorably to the learning event. The current mechanism for assessing an individual's reactions is through end of course surveys. Second, trainers assess “to what degree participants acquire the intended knowledge, skills, and attitudes based on their participation in the learning event” [23]. This is currently accomplished via formal testing mechanisms such as the end-of-course test completed by Airmen during BMT. Level 3 indicates “to what degree participants apply what they learned during training when they are back on the job” [23]. Supervisors of new officers and enlisted members

receive surveys asking them to rate the performance of the new member; however, the surveys are often AFSC specific. Unless the Airman is serving in a cyber related career field, there are no data points to indicate their cyberspace behavior. For the annual ADLS training, there is no mechanism to evaluate how the individuals are applying the training. Fourth, trainers need to determine “to what degree targeted outcomes occur, as a result of the learning event(s) and subsequent reinforcement.” The lack of targeted outcomes makes it difficult to determine the degree to which the training is achieving those outcomes.

## **2.5 Background Summary**

In summary, overall trainees receive initial training which consists of four hours of training for enlisted personnel, two hours for OTS and ROTC cadets and an unquantifiable number of hours for USAFA cadets. Additionally, all active duty members, both officer and enlisted, are required to complete 1.5 hours of training via ADLS annually. The methodology for developing, and assessing this training is ISD. Finally, it established the need for a pre and post baseline from which to evaluate the effectiveness of the training. The next chapter examines the approach to the research and presents the results of the research methodology.



### **III. Evaluation of Cyberspace Training**

#### **3.1 Approach**

This research uses a twofold approach. First, it applies inductive research to analyze the existing training and evaluation mechanisms. Second, it includes a survey mechanism to model the attitudes of individuals who have received the “Cyberspace and the Air Force” training.

As the developers of the “Cyberspace and the Air Force” curriculum, the AF CyTCoE requested an assessment of their curriculum. Specifically, they were interested in trainee’s reaction (Level 1) and to what degree targeted outcomes occur (Level 2). The initial plan was to develop a survey that could be used to evaluate these two areas and administer it to trainees at BMT. The survey would be administered to several flights of Airman pre-training and then administered again post-training. The results would guide curriculum developers as they prepared for the Triennial Review. According to Air Force Instruction 36-2201, *Technical and Basic Military Training Evaluation*, BMT will present evaluation data at the BMT Triennial Review [29]. The BMT Triennial Review is conducted not less than once every three years to review AF requirements for BMT graduate performance, military training, military studies, field training, curriculum course training standards, and other items of special interest identified by the Steering committee or other qualified sources [30].

The initial AF CyTCoE request to Air Education and Training Command A3TB resulted in direction to follow the Air Force Manpower process for requesting permission to conduct a survey. An alternative option was presented which included contacting the

Air Force Institute of Technology Air Force Learning Center (AFLC) representative for possible inclusion in the March 2012 AFLC. However, given the limited amount of time before the AFLC it was not likely to be included [31].

Once it was apparent that administering a survey to BMT trainees was not feasible in the time constraints of this research, a survey was developed to administer to First Term Airman stationed at Wright Patterson Air Force Base, Ohio. The First Term Airman Center is designed to assist new Airman at their first duty location as they transition from the training environment into the Air Force. While not ideal, administering a survey to this group afforded several opportunities. First, the demographic is very similar to the demographic attending BMT in that most of the participants fall in the 18-26 age range. Second, it offered a diversity of AFSCs. Finally, the procedures for obtaining permission to conduct the survey allowed completion of the survey within the time parameters of this research project.

### **3.2 Likert Survey**

A Likert survey is an established procedure for determining the attitudes and degree of the attitude of individuals in a particular area [32]. A Likert survey was chosen because understanding an individual's feeling towards a subject is critical to developing training that will transfer into the desired post training actions. Additionally, a Likert-Type Scale is listed as a viable option for conducting a pre-post evaluation in Air Force Manual 36-2236, *Guidebook for Air Force Instructor*. As such, Air Force personnel are familiar with this approach. This survey was not intended to measure the trainees

reaction to the specific “Cyberspace and the Air Force” training but to measure the overall perceptions or beliefs of the sample group.

The questions for the survey were based on the Cyber Wingman Philosophy since that was a common element to the BMT, OTS, ROTC, and USAFA training programs. This philosophy is the overarching cyber guidance provided by the Air Force on responsibilities and roles of all Air Force personnel. A five point scoring scale was chosen because it offers enough choices to measure the direction of the belief as well as indicate the strength of an opinion without too many options such that the surveyed individual cannot differentiate between the choices. A demographics section was included to verify the diversity of the population. It was important to understand the age range of the population and ensure there were a variety of different AFSCs. Finally, trainees were afforded the opportunity to provide open ended feedback at the end of the survey.

The survey questions (Appendix C) were designed to evaluate the individual’s beliefs in relation to fundamental Cyber Wingman Philosophy concepts (Appendix B). The survey is divided into 13 categories that cover all ten Cyber Wingman objectives (Appendix D). The subcategories are color coded to assist the reader in distinguishing between the different subcategories. Note that the colors should not be interpreted to infer any level of importance or other meaning.

1. The first subcategory identifies beliefs about how the Air Force uses cyberspace systems. Understanding how the Air Force uses cyberspace is essential to understanding why individuals need to secure and protect it.
2. The second subcategory identifies key cyberspace terms. Cyberspace training often includes terms such as threats and vulnerabilities. Understanding this terminology establishes the foundation for the desired

action. How do you ask someone to modify their behavior in order to reduce vulnerability if they do understand what constitutes vulnerability or if they perceive that no vulnerabilities exist?

3. The third subcategory was derived to measure a fundamental element of the Cyber Wingman Philosophy. Individuals are asked to secure cyberspace, but what are their beliefs concerning what constitutes a cyberspace system? Is cyberspace only a desktop computer at work?
4. Subcategory 4 was designed to gauge an individual's perception about what is a threat to a cyberspace system.
5. Subcategory 5 was written to directly measure perceptions compared to Cyber Wingman Principle 2: "Our adversaries plan malicious code, worms, botnets and hooks in common Web sites, software and in hardware such as thumbdrives, printers, etc."
6. Subcategory 6 was designed to determine individual beliefs concerning the consequences of a breach. Why would someone work diligently to practice good cyber principles if they do not believe there are consequences for failing to do so?
7. While the Clausewitz's quote "know your enemy, know yourself" may be overused, the principle holds true. One must recognize an adversary's motivations to defend against them. Subcategory 7 was designed to determine how individuals perceive the adversaries motives.
8. Many Air Force members often take their work home with them. As such, subcategory 8 was developed to test individual's beliefs concerning how to properly transfer information from a government system to their personal systems. It also seeks to measure their beliefs concerning how actions on personal systems can impact Air Force systems.
9. The Cyber Wingman Philosophy, as well as Air Force Information Assurance Awareness training, emphasizes the need for individuals to protect their Personally Identifiable Information (PII). How does a generation who grew up posting information on Facebook, Twitter, and other social media perceive what constitutes personal information? Subcategory 9 was developed to test beliefs concerning what constitutes an individuals' PII.
10. Subcategory 10 directly correlates to Cyber Wingman Principle 7: "Do not open attachments or click on links unless the email is digitally signed, or you

can directly verify the source, even if it appears to be from someone you know.”

11. Cyber Wingman Principle 8 is an action item versus a knowledge level item. It seeks for individuals to behave in a certain manner. Subcategory 11 was intended to capture beliefs concerning downloading or using applications and software. Most individuals are more likely to modify their behavior if they believe the new behavior is organizationally acceptable behavior.
12. Subcategory 12 relates to an understanding of what constitutes classified or sensitive information, a critical element to behaving in accordance with Cyber Wingman Principle 9.
13. Finally, Subcategory 13 directly correlates to Cyber Wingman Principle 10: “Install the free Department of Defense anti-virus software on your home computer. Your CSA can provide you with your free copy or click here to see download sites.” Individuals will most likely fail to perform the desired action, install anti-virus software on their home computer, if they do not believe this is a permitted action.

The following guidance was provided to the Airmen prior to administering the survey: “In February 2010, Air Education and Training Command tasked the Air Force Technical Center of Excellence to develop cyberspace curriculum for inclusion in BMT. The curriculum was delivered in August 2010 and the first Airmen received the training graduated in October 2010. Since the training is now a year old, the Center would like to conduct a review to determine if the current course material is meeting Air Force needs. The purpose of this study is to evaluate the ‘Cyberspace and the Air Force’ curriculum currently being provided during Air Force BMT. Additionally, the survey will be used by an Air Force Institute of Technology Graduate Student to complete their Graduate Research Project. This survey is completely voluntary and you may elect not to participate at any time. There will be no adverse actions taken against you for choosing not to participate in this survey. For each statement on the survey, please fill in the circle

for the number that indicates the extent to which you believe the statement is true. There is a short demographic section following the questions. These items will be used for statistical purposes only and will not be used to identify individual responses. Thank you very much for your time and participation.” The survey was submitted through the Air Force Institute of Technology Institutional Review Board process and approved for exemption from the human experimentation requirements.

### **3.3 Survey Demographics**

This section presents the results of the Likert survey demographics information (Appendix C, Section 2). The survey was administered on two separate occasions to Airmen at the Wright Patterson Air Force Base First Term Airman Center. A total of 33 individuals participated in the survey. The group consisted of 24 males and 9 females. Only two of the 33 individuals indicated they were 27+ years old and all fall within the previously defined definition of Millennial. This sampling included 15 different AFSCs which are summarized in Table 1 below. It should be noted that five of the individuals are from cyber related career fields. This is significant since one individual commented “much of what I learned pertaining to this subject matter I remember being taught in technical school. As far as to remember learning this same information in BMT I cannot fully recall.”

**Table 1 AFSCs Surveyed**

<b>AFSC</b>	<b>Title</b>	<b>Total</b>
9S100	Scientific Applications Specialist	7
3P0X1	Security Forces	6
4NOX1	Aerospace Medical Service	5
3D0X1 *	Knowledge Operations Management	2
3D1X2 *	Cyber Transport Systems	2
4C0X1	Mental Health Service	2
1C1X1	Air Traffic Control	1
1N1X1	Geospatial Intelligence	1
1N2X1	Signals Intelligence Analyst	1
3D0X4 *	Computer Systems Programming	1
3N0X1	Public Affairs	1
3N1X1	Regional Band	1
3S0X1	Personnel	1
4E0X1	Public Health	1
4R0X1	Diagnostic Imaging	1
		<b>33</b>

\* Indicates cyber related career field

The demographics requested ASVAB scores; however, there were an insufficient number of responses to this question to draw meaningful conclusions. All of the responses received were from Active Duty enlisted Air Force members. Finally, individuals were asked to rate their level of computer experience prior to joining the Air Force. The samples provided were not formal criteria used by the Air Force, but rather an attempt to capture the individual's comfort level using various cyberspace technologies. Four individuals rated themselves as "experienced", 25 chose "some experience" and four selected "beginner experience." Individuals were given the opportunity to provide open-ended feedback at the conclusion of the survey. Only two respondents elected to provide comments. The first was the aforementioned statement "much of what I learned pertaining to this subject matter I remember being taught in technical school. As far as to remember learning this same information in BMT I cannot fully recall." The second

comment was “Some of the training was a little to repetitive and could be spent learning other cyberspace security methods or become more hands on.”

### **3.4 Results of the Likert Survey**

What became known as the Likert method of attitude measurement was formulated by Rensis Likert, and first appeared in an abridged version in a 1932 article in the Archives of Psychology. At the time, many psychologists felt their work should be confined to the study of observable behavior [32]. Since its inception, there has been considerable debate concerning how to interpret the data collected from a Likert survey. In statistical terms, these objections amount to arguing that the level of measurement of the Likert scale is “ordinal” rather than “interval.” This means one may make assumptions about the order but not the spacing of the response options [32]. The responses to this survey are presented in two different formats. First, Appendix E presents the summation value and the mean value response for each question. The results are presented in this manner because it is the most common approach for presenting the results of Likert Surveys and most people are comfortable with summation and mean statistics. However, given the controversy associated with using the mean approach with ordinal numbers and claiming the sample population has a 3.13 mean belief that the Air Force uses cyberspace for conducting fire protection is not completely institutive, the results are also presented in a second format that shows the number of individual responses to each question (Appendix F).

The following is a synopsis of key points of the survey results:

- Subcategory 1 shows that Airmen understand that the Air Force uses cyberspace for many different types of operations. There was a strong belief



that that Air Force uses cyberspace for intelligence, surveillance and reconnaissance operations; as well as remotely piloted aircraft operations. They were also aware of areas where cyberspace was not heavily integrated and do not conclude cyberspace is heavily entwined in all operations.

- Subcategory 2 indicated that Airmen are not certain about the definition of key cyberspace terms. While there was a strong belief concerning the definition of cyberspace vulnerability, they were more neutral concerning the definitions of a cyberspace risk and social engineering. Often times trainers and briefers use these terms believing the audience understands the nuances of the various definitions. Establishing a common vernacular is essential to communicating policy and expected behavior.
- Subcategory 3 demonstrates that Airmen understand that cyberspace security principles apply across a variety of systems, to include government and personal systems.
- Subcategory 4 indicates that the Airmen surveyed understood that threats to Air Force cyberspace systems stem from a variety of actors; such as, insider threats, criminal organizations, and individual hackers. It is worthwhile to note that the National Security Agency and Federal Bureau of Investigation were scored near neutral as a threat to Air Force cyberspace systems. This would be a definite area for more in-depth attitude analysis.
- Subcategory 5 showed that the Airmen believed “Planting malicious code, worms, or botnets in common websites, software, or hardware is one method for exploiting USAF networks.”
- Subcategory 6 indicates that Airmen comprehend the potential consequences of a breach to cyberspace security. They believe that intrusions can result in more than the loss of data.
- Subcategory 7 suggests that Airmen understand there a variety of motivations of attacking Air Force cyberspace systems. They do not perceive the motivation as being limited to state actors and traditional espionage.
- Subcategory 8 points out that Airmen understand that information they post on social media is valuable to adversaries. However, responses to questions concerning the transfer of information from a government system to a personal system suggest they do not believe there is a proper method for transferring information. Ensuring individuals understand the correct protocol enables them to conduct their work in a safer manner.

- Subcategory 9 points towards a lack of understanding when it comes to PII. In order to protect PII, individuals must recognize the information as worthy of protection. This is a prime area for further investigation and increased emphasis in training.
- Subcategory 10 denotes that Airmen realize the risks associated with opening attachments or clicking on links from individuals they do not know. The next series of questions would be to determine if this belief influences their actions and how they determine the identity of someone online.
- Subcategory 11 points toward an uncertainty concerning the use of social media and games on Air Force systems. While policy and guidance on the use of social media on Air Force networks exists, the survey indicates Airmen may not fully understand the directives.
- Subcategory 12 signifies that Airmen understand that classified information posted via a public forum (e.g., Wikileaks) remains classified. The next series of questions related to this area would explore how Airmen respond to a situation where they find classified information posted on a public website. As demonstrated by Wikileaks, there is a need for military members to understand the rules pertaining classified information and public websites.
- Subcategory 13 indicated that members do not believe they are permitted to install free Department of Defense anti-virus software on their home computers. Since this is one of the “do” items from the Cyber Wingman Philosophy, it is worthwhile to examine the belief. Airmen will not perform the desired action if they do not perceive it is permissible.

### **3.5 Evaluation of Cyberspace Training Summary**

This chapter outlined the rationale for choosing a Likert Survey as the methodology for this research. Since the survey could not be administered at BMT due to timing and approval constraints, it was provided to First Term Airmen at Wright Patterson Air Force Base, Ohio. Next, the development of survey questions, establishment of survey subcategories, and demographics portion of the survey were discussed. The results of the demographic information were discussed in order to establish a baseline for presentation of the survey results. Finally, the section concluded by presenting the results of the

survey in three formats: summation, average, and response per question. It also provided a brief synopsis of the finding for each subcategory. The next chapter focuses on the analysis and recommendations of this research.

## **IV. Analysis and Recommendations**

### **4.1 Determine the Objective of the Training**

An analysis of the inductive research and the Likert survey reveal a need to determine the overall objective of cyberspace training. Is the goal of Air Force cyberspace training to influence attitudes, elicit specific behaviors or increase user awareness through the delivery of information? According to the *Guidebook for Air Force Instructor* “Too often, instruction is limited to the delivery of information, either through reading assignments, lectures, films, or type-0 and type-1 computer-based training. Academic instruction should allow adult learners to practice what has been taught, receive feedback on their performance, and incorporate improvements.” The Guidebook goes on to state “In the approach presented in this manual, the only acceptable evidence that successful teaching has taken place comes from indications of change in student behavior” [33]. While each cyberspace training program lists the objectives for the training, there is a need for an overarching Air Force cyberspace training objective to guide the curriculum developers.

The “Rise of the Cyber Wingman” Philosophy (Appendix B) includes four items where Airmen are expected to behave in a certain manner: (i) Do not open attachments or click on links unless the email is digitally signed, or you can directly verify the source; (ii) Do not connect any hardware or download any software, applications, music or information onto Air Force networks without approval; (iii) Encrypt sensitive but unclassified and/or mission critical information, and (iv) Install the free Department of Defense anti-virus software on your home computer [3]. Clearly, the Air Force intends for Cyber Wingman to go beyond a mere understanding of cyberspace threats and

vulnerabilities and to behave in a manner that helps protect and defend Air Force networks and information. However, the stated objective in the “Cyberspace and the Air Force” Plan of Instruction is “Identify basic facts about operating within the Cyberspace Domain” [34]. Finally, the listed objectives for the annual ADLS training “Information Protection provides general awareness level training for Information Security, Privacy Act, Freedom of Information, NATO Security subjects and basic Operational OPSEC principles.” The stated objective of Information Assurance Awareness training is “DoD Information Assurance Awareness training will address the following main objectives (but not limited to): the importance of IA to the organization and to the authorized user; relevant laws, policies, and procedures; examples of external threats; examples of internal threats; how to prevent self-inflicted damage to system information security through disciplined application of IA procedures; prohibited or unauthorized activity on DoD systems; categories of information classification and differences between handling information on the NIPRNet or SIPRNet; requirements and procedures for transferring data to/from a non-DoD network” [35]. From these three examples, it is apparent that there is not a clearly defined or well understood objective.

In addition to establishing the objective, the Air Force should outline what types of materials should be included in cyberspace training. Does cyberspace training include information assurance, or should information assurance constitute separate training? BMT training includes Information Assurance training in the “Cyberspace and the Air Force” lesson. Officer Training School and ROTC separate this into two separate blocks of instruction. Finally, ADLS is focused more on information protection and information assurance and does not detail Air Force uses of cyberspace. Part of establishing the

objective of cyberspace training is to determine where information assurance fits in the context of the cyberspace structure.

Once the requirements are established, a core module of cyberspace training should be taught at BMT, USAFA, ROTC, and OTS. The AF CyTCoE is a rational place to develop a core module that is presented at each of these institutions. This core module should include all aspects the Air Force deems necessary for responsible behavior on an Air Force network. Building upon the Cyber Wingman Philosophy, which is included in all the initial training programs, is a logical place to start. If the training program desires to implement additional training beyond this, they may. For instance, USAFA and ROTC detachments may choose to incorporate more training since they have years versus weeks. Although some may counter that this already exists in the “Information Assurance Awareness” training that everyone must complete prior to accessing a Department of Defense network, if “Information Assurance Awareness” is fulfilling this requirement then why are the dollars and man-hours spent on additional cyberspace training? Once again, there is strong rationale for establishing the objective of cyberspace training.

#### **4.2 Establish the Baseline**

Once the training objective is established, there is a need to establish a pre and post training attitude assessment. This principle is already recognized by the Air Force and outlined in the *Guidebook for Air Force Instructors*. The Guidebook provides several options for conducting the assessment: using published attitude scales, using a commercially published attitude scale, or developing an organic attitude assessment scale

[33]. According to the guidebook, the most widely used strategy in affective measurement is the pre-test/post-test design. In this design, students' attitudes are measured at one point in time to determine their attitudes before instruction. Students are then exposed to some learning experience and after the activity, attitudes are again measured and the results compared to those obtained in the pre-test [33].

There are many different ways to accomplish the assessment. The first course of action is to administer the survey to all individuals as part of their initial military in-processing. For enlisted members, this could be accomplished at the Military Entrance Processing Station and add no additional burden to BMT instructors. Members could then receive the post-survey as part of the end of course survey. If it is deemed this is too grand of a scale and the Air Force does not have the resources to track 40,000+ surveys, leverage the personnel developing the curriculum, AF CyTCoE, could administer the survey quarterly to trainees at BMT. The same type survey could be administered to individuals throughout their career to evaluate the effectiveness of annual ADLS training. A quick survey prior to beginning the training and another before the member receives their training certificate of completion.

An attitude assessment offers many advantages. First, it allows curriculum developers to focus their lesson plans so they can identify attitudes they wish to influence and avoid time on attitudes that already conform to the desired objective. For instance, the results of the Likert Survey in this research indicates that Airman understand the consequences of breaches to Air Force systems. However, their attitudes concerning what constitutes PII may be an area for additional emphasis. Second, it provides the Air Force with a more useful mechanism for assessing the return on investment for

cyberspace training. All active duty members are required to complete 30 minutes of Information Protection training and 60 minutes of Information Assurance Awareness training annually. If you multiply 328,871 active duty members [26] times 90 minutes of training, that is over 493,306 hours of cyberspace training completed annually. For this level of investment, there should be a measureable return. Finally, understanding Airmen's attitudes allows the Air Force to develop and articulate specific policy and guidance. For example, the Likert Survey administered as part of this research revealed that the surveyed Airmen were unclear on the appropriate use of social media on Air Force networks. Leadership can use this as a data point to determine if the existing policy needs to be refined or articulated in a more effective manner.

#### **4.3 Involve Curriculum Developers in the Process**

Perhaps the most predominate requirement identified in this research is the need to incorporate personnel involved in curriculum development in the review and update process. There is currently no feedback being provided to the developers of the "Cyberspace and the Air Force" curriculum. Additionally, no evidence was discovered to indicate feedback is being provided to the original customer, Air Force Space Command. Members of the AF CyTCoE delivered the lesson plan to the 737th Training Group in August 2010 and the first individuals received the training in October 2010 [5]. Since that time there has been no formal feedback provided to the AF CyTCoE staff, to include comments from trainees, statistics related to how trainees were performing on the end of course written exam, identification of high missed questions, or trainees' failures to meet objectives. Additionally, AF CyTCoE has never observed the instructors delivering the



lesson plan to validate if it was delivered as they intended during the development. This observation could be conducted with minimal interruption to trainees and instructors by either streaming a video of instructors during lesson presentation or by having the presenters record one of the lessons and mail it to AF CyTCoE. Although the AF CyTCoE has requested feedback many times, they have been unable to obtain the requested information. Likewise, all requests for visitations to observe the training have been denied. The researcher submitted a request to AETC/A3TB for any received feedback from trainees concerning their reaction to this block of training. After researching the feedback, AETC/A3TB indicated most comments from trainees were related to MTIs and daily life during BMT and there were no specific comments related to this block of training.

The 737 TRS maintains metrics on end of course tests and has the capability of identifying high missed questions but this does not necessarily translate to improvements in the overall lesson plan. The 737 TRS is responsible for presenting the lesson to the trainees and they deliver what is provided to them in the lesson plan. To have truly effective training, there needs to be a symbiotic relationship between those developing the lesson and those teaching the lesson. As the developers of the curriculum, the AF CyTCoE must be involved in the process to provide enhanced lesson plans.

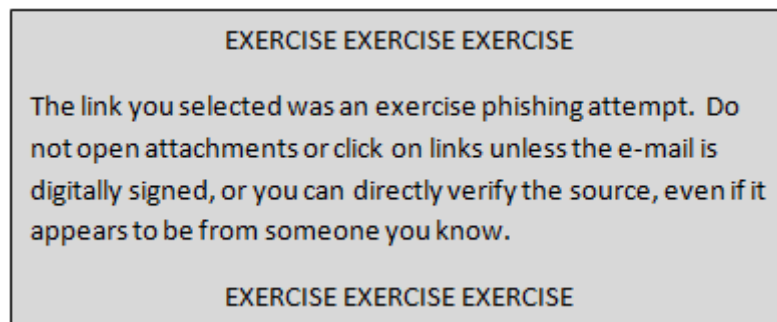
The Triennial Review process is the venue for adding or removing training from the overall BMT curriculum [19]. Since the “Cyberspace and the Air Force” training is already established, it now falls into the maintenance category. Unless there is a 20% change in the course context, there is no need for the training to be evaluated during the Triennial Review process. This excludes minor typographical or grammatical

corrections, and minor plan of instruction, lesson plan, study guide/workbook, or measurement device technical additions or deletions [19]. Therefore, if the lesson developers are included in the process they have the ability to update the quality of the training as long as they are not altering the course content or length by more than 20%. They could change the vignettes, address new or emerging threats, and address areas identified in the attitude assessment if provided proper feedback. Similar processes and standards apply to USAFA, OTS, ROTC, and ADLS training. The current system is sufficient for providing updates to the training if the developers are included in the process.

#### **4.4 The Need for Feedback**

The need for feedback extends beyond the course developers. According to the *Guidebook for Air Force Instructor* “For efficient instruction, students need feedback that reinforces instruction,” additionally it states “Too often, instruction is limited to the delivery of information, either through reading assignments, lectures, films, or type 0 and type 1 computer-based training.” Academic instruction should allow adult learners to practice what has been taught, receive feedback on their performance, and incorporate improvements. For effective cyberspace training, there must be feedback to the user. Trainees would greatly benefit from interactive training. In this regard, training similar to that provided in the ADLS “Information Assurance Awareness” training would be effective. Instead of merely presenting individuals with a list of PII, show them a sample Social Media page and have them identify the PII listed on the page.

This feedback must extend beyond the training classroom and into everyday experience and exercises. Many Air Force members can relate to this scenario: You have a base exercise and during the exercise you are told 20 personnel clicked on an unauthorized exercise phishing link. However, no feedback is provided to the 20 people to explain their error to them. Consider the same exercise with an individual that ventures outdoors during a Tornado Warning. The individual is immediately stopped by an evaluator and told they must remain indoors during Tornado Warnings. In this case, they are provided the immediate feedback that is necessary to reinforce their academic training. They are provided the opportunity to practice what has been taught, receive feedback on their performance, and incorporate improvements. This same principle needs to be applied to cyberspace training. This relates to the original finding of the need to establish the objective of cyberspace training. When the exercise phishing message is sent out, design it so the individual is presented a dialog box indicating the error when they click on the link. Like the Tornado scenario, the individual receives immediate feedback to reinforce the training and results can be recorded without identifying specific personnel during the exercise out brief. Figure 5 presents one possible example of a dialog box that users could receive.



**Figure 5 Sample Exercise Message**

Is it enough that the user is aware that phishing attacks exist or is the requirement for the user to apply that knowledge into every day operations? If it is the former, then the current mechanisms for providing feedback on cyberspace training are adequate. If the objective is application of the knowledge, the feedback mechanisms are woefully inadequate.

#### **4.5 The Illusion of Progress Can Be Dangerous**

According to Jim and Wendy Kirkpatrick, trainers must be cautious to avoid checkmark training. They use this term to refer to measuring the value of training based on consumptive metrics, including the number of courses available and the number of hours of training completed [36]. There is a great danger in developing training and declaring victory without properly evaluating the effectiveness of the training. The illusion of well trained cyber users can lead to a failure to provide adequate security, policy, protection, and defense mechanisms. Understanding user attitudes and capabilities allows those charged with developing and defending Air Force networks and those charged with providing cyberspace mission assurance to better perform their mission.

The following scenario illustrates this point. A couple with two young children wants to purchase a new sofa. Since their children are young, they assess the risk of having spills and stains as high. Consequently, they elect to purchase additional stain protectant and have their sofa treated before it is delivered to their house. As the children grow, they learn to be cautious with their drinks and the number of spills decreases. When the couple returns to purchase a sofa some years later, they assess the risk of spills and stains

as much lower. After all, the children have learned how to take precautions to prevent accidents from happening. The couple realizes that accidents may still occur but the likelihood is greatly decreased. Therefore, the couple chooses not to purchase additional stain protectant for their sofa. They are able to apply the money for stain protectant to a different purchase. The same principle applies to Air Force cyberspace training. If the Air Force assesses the likelihood of cyberspace breaches caused by user actions as high, then it is worthwhile to invest in additional protection measures. However; if the assessment concludes that the likelihood of cyberspace breaches caused by user actions as low, the additional funds and security measures can be applied to other areas. The strategy is driven by the objectives and effectiveness of cyberspace training.

#### **4.6 Analysis and Recommendations Summary**

This section highlighted the overwhelming need to establish clearly defined objectives for Air Force Foundational Cyberspace Training. The absence of clearly stated objectives directly influences many of the recommendations. Additionally, the analysis showed that completion of an attitude assessment would benefit curriculum developers, provide a useful mechanism for assessing the return on investment for cyberspace training, and allow the Air Force to develop and articulate specific cyberspace usage policy and guidance. Moreover, the analysis and recommendations identified the need for inclusion of curriculum developers in the process and the importance of providing feedback to both curriculum developers and cyberspace users. The chapter concluded with a caution about gauging the effectiveness of training based on number of

courses or hours spent on training. The next chapter discusses the impacts of this research, limitations of this work, and offers areas for further studies.

## **V. Conclusions**

### **5.1 Impact on the Air Force**

This research offers three significant impacts for the Air Force. First and foremost, it offers the potential for savings in man-hours and dollars spent on training. Implementing the recommendation to standardize training into a core module that is presented to both enlisted and officer trainees as they enter the Air Force reduces redundancy and duplication of effort in developing curriculum for separate institutions: BMT, USAFA, ROTC, and OTS.

Second, using the results of the Likert survey to assess Airmen's attitudes can assist curriculum developers in writing training plans that are more applicable to user's needs. The survey can be used to identify areas where trainee's perceptions are already congruent with Air Force principles and those areas that need additional focus. This allows the authors to focus the training where it is needed. This study provides an initial assessment but more exhaustive research is needed.

Third, it identifies a critical lack of feedback to both the curriculum developers and the users. Identifying this lack of feedback provides an opportunity for the Air Force to correct the situation without a significant investment of resources. There is very little cost associated with developing a more cohesive relationship between those developing the training and the cadre who delivers the training. Additionally, any unit conducting an exercise that involves cyberspace users can have evaluators to provide direct feedback to the individuals with very few additional man-hours.

## **5.2 Limitations of this Work**

This research is limited to training that is formally recognized and mandated by the Air Force. The research focused only on those programs that are intended for all members of the Air Force. Training for cyberspace specific specialty codes, unit level, and training provided during Professional Military Education was not included in this research. This survey was limited to Active Duty members of the Air Force. Members of the Air National Guard, Air Force Reserves, and Air Force civilians were not addressed.

There were limitations associated with the development and administration of the Likert Survey. First, the Likert survey needs to be administered to a pre-training and post-training group. While the survey is useful for addressing Airmen's current attitudes, it is not sufficient for determining the effectiveness of the training. Second, the post-training needs to be accomplished soon after the training. As mentioned by one member during the survey, it is difficult to determine what learning occurred as a result of the BMT training when the member has experienced additional training events after that training. Finally, the sample size for the survey must be much larger. Given that 30,000 - 40,000 members at BMT, 4,000+ cadets at USAFA, 2,400+ OTS cadets, and 1,800+ ROTC cadets receive introductory cyberspace training the sample size for the Likert survey is insufficient for drawing wide-ranging conclusions.

## **5.3 Areas for Future Study**

This research highlighted many areas for future study. One area for future research is identifying the entering attitudes and knowledge level of members joining the Air Force.



While there are studies concerning Millennials use of cyberspace, most of the research is focused on hours used, types of devices used, and how they are used. None of these are applicable to determining attitudes related to Air Force operating principles. A second area for research is to conduct a pre and post training analysis. There is a need to determine the return on investment for training. A third potential area would be to conduct a comparison of Air Force users to the average civilian user. For example, how does the cyber security awareness of the average Air Force user compare to the standard American citizen? A fourth area for research is to determine what information or topics should be included in the “Cyberspace and the Air Force” core module. Finally, there is a need to define what is meant by cyberspace training. Is it Information Assurance, Mission Assurance, a combination of the two, or something entirely different?

#### **5.4 Closing Thoughts**

The Air Force has been at the forefront of cyberspace operations. The addition of cyberspace to the Air Force mission statement was the first of many steps to recognize the critical importance cyberspace plays in military operations and national defense. All users with access to Air Force networks have a responsibility to behave responsibly and to protect and defend those systems. Recognizing this fact, the Air Force instituted cyberspace training to help prepare all members to be responsible cyber users. The next step in the Air Force’s cyberspace development is to determine the effectiveness of the training. It is not sufficient to simply implement training. The training must be continuously evaluated and feedback provided to the curriculum developers in order to develop outstanding training and achieve the desired cultural changes. Cyberspace is

critical to successful operations and the Air Force must ensure the quality of the training must mirrors the importance of the mission.

## Appendix A - Letter to Airmen 2005



THE SECRETARY OF THE AIR FORCE  
CHIEF OF STAFF, UNITED STATES AIR FORCE  
WASHINGTON DC



DEC 07 2005

To the Airmen of the United States Air Force.

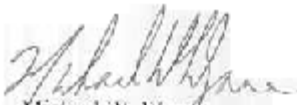
Almost 60 years ago the President and Congress created our Air Force. The world we live in today has changed dramatically over those six decades. Today, our world is fast paced, constantly shifting, and filled with a wide range of challenges. Our mission is our guiding compass, and now more than ever we need it to be clear and precise. Therefore, we have rewritten the Air Force's mission statement to define where and what we do...

*The mission of the United States Air Force is 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.*

Our task is to provide the National Command Authority, the Combatant Commanders, and our Nation with an array of options ... options that are not limited by the tyranny of distance, the urgency of time, or the strength of our enemy's defenses. With one hand the Air Force can deliver humanitarian assistance to the farthest reaches of the globe, while with the other hand we can destroy a target anywhere in the world. This is the meaning of sovereign options and the essence of being a superpower. We will be the best at what we do, and we will accomplish our mission as part of a joint, coalition team.

Our adversaries will contest us across all of the domains: Land, Sea, Air, Space, and Cyberspace. As Airmen, it is our calling to dominate Air, Space, and Cyberspace. If we can decisively and consistently control these commons, then we will deter countless conflicts. If our enemies underestimate our resolve, then we will fly, fight, and destroy them.

The pioneers of airpower - Billy Mitchell, Hap Arnold, Curtis LeMay, Bernard Schriever - knew what their mission was: to fly and fight wherever our Nation calls. The Air Force's mission statement has evolved over time, but it does not change the nature of who we are or what we do. Our heritage has given us a limitless horizon. Just as our predecessors did in the past, we will continue to fly, to fight, and to win wherever we are called. We are the greatest Air Force in the world, because of you ... because of your sacrifice, dedication, and skill. Keep up the great work!

  
Michael W. Wynne  
Secretary of the Air Force

  
T. Michael Moseley  
General, USAF  
Chief of Staff

[1]

## **Appendix B - Rise of the Cyber Wingman**

**The "Rise of the Cyber Wingman" philosophy incorporates the following 10 guiding principles every Airman needs to know and use to secure cyberspace.**

1. The United States is vulnerable to cyberspace attacks by relentless adversaries attempting to infiltrate our networks -- at work and at home -- millions of times a day, 24/7.
2. Our adversaries plant malicious code, worms, botnets and hooks in common Web sites, software and in hardware such as thumbdrives, printers, etc.
3. Once implanted, this code begins to distort, destroy and manipulate information, or it "phones" it home. Certain code allows our adversaries to obtain higher levels of credentials to access highly sensitive information.
4. The adversary attacks your computers at work and at home knowing you communicate with the Air Force network by e-mail or by transferring information from one system to another.
5. As cyber wingmen, you have a critical role in defending your networks, your information, your security, your teammates and your country.
6. You significantly decrease our adversaries' access to our networks, critical Air Force information, and even your personal identity, by taking simple action.
7. Do not open attachments or click on links unless the email is digitally signed, or you can directly verify the source, even if it appears to be from someone you know.
8. Do not connect any hardware or download any software, applications, music or information onto Air Force networks without approval.
9. Encrypt sensitive but unclassified and/or mission critical information. Ask your computer security administrator, or CSA, for more information.
10. Install the free Department of Defense anti-virus software on your home computer. Your CSA can provide you with your free copy or click [here](#) to see download sites.

[3]

## Appendix C – Likert Survey

### ‘Cyberspace and the Air Force’ Survey

The purpose of this survey is to support research for an Air Force Institute of Technology Graduate Research Project and to aid the Air Force Technical Center of Excellence in evaluating the curriculum being provided in the ‘Cyberspace and the Air Force’ training. This survey is completely voluntary and you may elect not to participate at any time. There will be no adverse actions taken against you for choosing not to participate in this survey.

For each statement, please fill in the circle for the number that indicates the extent to which you believe the statement is true. Use the scale below for your responses.

	④ Strongly Disagree	③ Disagree	② Neither Agree or Disagree	① Agree	⑤ Strongly Agree
1. USAF uses cyberspace for conducting fire protection	①	②	③	④	⑤
2. USAF uses cyberspace for vehicle maintenance control	①	②	③	④	⑤
3. USAF uses cyberspace for operating remotely piloted aircraft (RPA)	①	②	③	④	⑤
4. USAF uses cyberspace for sending e-mails/surfing web	①	②	③	④	⑤
5. USAF uses cyberspace for conducting intelligence, surveillance and reconnaissance operations	①	②	③	④	⑤
6. A cyberspace vulnerability is a weakness in an information system or system security procedures that can be exploited	①	②	③	④	⑤
7. Employees are a potential threat to USAF cyberspace operations	①	②	③	④	⑤
8. Criminal organizations are a potential threat to USAF cyberspace operations	①	②	③	④	⑤
9. Individuals or small groups are a potential threat to USAF cyberspace operations	①	②	③	④	⑤
10. The National Security Agency (NSA) is a potential threat to USAF cyberspace operations	①	②	③	④	⑤
11. The Federal Bureau of Investigation (FBI) is a potential threat to USAF cyberspace operations	①	②	③	④	⑤
12. A potential motive for exploiting USAF cyberspace systems is to gather intelligence or commit espionage	①	②	③	④	⑤
13. A potential motive for exploiting USAF cyberspace systems is to conduct counter narcotic operations	①	②	③	④	⑤
14. A potential motive for exploiting USAF cyberspace systems is to access intellectual property	①	②	③	④	⑤
15. A potential motive for exploiting USAF cyberspace systems is to disrupt USAF systems or operations	①	②	③	④	⑤
16. A cyberspace vulnerability is a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of the occurrence	①	②	③	④	⑤
17. Planting malicious code, worms, or botnets in common websites, software, or hardware is one method for exploiting USAF networks	①	②	③	④	⑤

	① Strongly Disagree	② Disagree	③ Neither Agree or Disagree	④ Agree	⑤ Strongly Agree
18. Social engineering is an attempt to trick someone into revealing information that they would not normally reveal	①	②	③	④	⑤
19. Failure to secure USAF cyberspace systems could result in adversaries gaining information about USAF current and future operational plans	①	②	③	④	⑤
20. Failure to secure USAF cyberspace systems could result in the loss of USAF technological advantages	①	②	③	④	⑤
21. Failure to secure USAF cyberspace systems could result in the loss of command, control, and communications capabilities	①	②	③	④	⑤
22. Cyberspace security principles apply when operating your smart phone	①	②	③	④	⑤
23. Cyberspace security principles apply when operating on a USAF network	①	②	③	④	⑤
24. Cyberspace security principles apply when operating on your home computer or private network	①	②	③	④	⑤
25. Your gender is considered Personally Identifiable Information (PII) and should be protected	①	②	③	④	⑤
26. Your military rank is considered Personally Identifiable Information (PII) and should be protected	①	②	③	④	⑤
27. Your job description is considered Personally Identifiable Information (PII) and should be protected	①	②	③	④	⑤
28. Your cellular phone number is considered Personally Identifiable Information (PII) and should be protected	①	②	③	④	⑤
29. An adversary can gain valuable information from information you post on social media, like Facebook or Twitter	①	②	③	④	⑤
30. If you see classified information on a public website, it is acceptable to download it because once information is posted on a public site it is no longer classified	①	②	③	④	⑤
31. On a USAF network, it is acceptable to open an attachment from someone you do not know as long as you run it through a virus scanner prior to opening it	①	②	③	④	⑤
32. You can install free Department of Defense anti-virus software on your home computer	①	②	③	④	⑤
33. It is acceptable to download games listed on a USAF network as long as they are on the USAF 'Approved Gaming' list	①	②	③	④	⑤
34. You should never click on a link in an e-mail unless the e-mail is digitally signed or you can directly verify the source	①	②	③	④	⑤
35. You are allowed to use a thumbdrive to transfer information from a USAF computer to your home computer	①	②	③	④	⑤
36. You are allowed to burn information to a CD to transfer information from a USAF computer to your home computer	①	②	③	④	⑤
37. You are allowed to use Social Media, such as Facebook or Twitter, on a USAF network	①	②	③	④	⑤

**Section 2 (Demographics):** This section contains items regarding your personal characteristics. These items will be used for statistical purposes only and will not be used to identify individual responses.

Respond to each item by **WRITING IN THE INFORMATION** requested or **CHECKING THE BOX** ☒ that best describes you

1. What is your gender?

- ☐ **Male**  
☐ **Female**

2. What is your age based on the ranges listed below?

- ☐ **18 – 24**  
☐ **25 – 27**  
☐ **27 +**

3. What is your AFSC (if unknown leave blank)? \_\_\_\_\_

4. What is your ASVAB Score (if unknown leave blank)

<b>AFQT</b>	_____
<b>General</b>	_____
<b>Mechanical</b>	_____
<b>Administrative</b>	_____
<b>Electrical</b>	_____

5. Air Force Component

- ☐ **Active Duty**  
☐ **Air National Guard**  
☐ **Air Force Reserve**

6. Prior to joining the United States Air Force (USAF) how much computer experience did you have?

- ☐ **Beginner Experience (I Surf the Web, send e-mails, tweet my friends)**  
☐ **Some Experience (I had computer classes in school or can do more than a beginner)**  
☐ **Experienced (I can write or know how to conduct a buffer overflow)**

**Thank you for your participation!**

**Please include any comments you have**

## Appendix D – Likert Subcategories

Question Number	Question	Subcategory
1	USAF uses cyberspace for conducting fire protection	1 - AF Use of Cyberspace
2	USAF uses cyberspace for vehicle maintenance control	1 - AF Use of Cyberspace
3	USAF uses cyberspace for operating remotely piloted aircraft (RPA)	1 - AF Use of Cyberspace
4	USAF uses cyberspace for sending e-mails/surfing web	1 - AF Use of Cyberspace
5	USAF uses cyberspace for conducting intelligence, surveillance and reconnaissance operations	1 - AF Use of Cyberspace
6	A cyberspace vulnerability is a weakness in an information system or system security procedures that can be exploited	2 - Key Terms
16	A cyberspace vulnerability is a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of the occurrence	2 - Key Terms
18	Social engineering is an attempt to trick someone into revealing information that they would not normally reveal	2 - Key Terms
22	Cyberspace security principles apply when operating your smart phone	3 - Wingman Principle 1 - ID cyberspace systems
23	Cyberspace security principles apply when operating on a USAF network	3 - Wingman Principle 1 - ID cyberspace systems
24	Cyberspace security principles apply when operating on your home computer or private network	3 - Wingman Principle 1 - ID cyberspace systems
7	Employees are a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace
8	Criminal organizations are a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace
9	Individuals or small groups are a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace
10	The National Security Agency (NSA) is a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace
11	The Federal Bureau of Investigation (FBI) is a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace
17	Planting malicious code, worms, or botnets in common websites, software, or hardware is one method for exploiting USAF networks	5 - Wingman Principle 2
19	Failure to secure USAF cyberspace systems could result in adversaries gaining information about USAF current and future operational plans	6 - Wingman Principle 3 - Consequences of breeches
20	Failure to secure USAF cyberspace systems could result in the loss of USAF technological advantages	6 - Wingman Principle 3 - Consequences of breeches
21	Failure to secure USAF cyberspace systems could result in the loss of command, control, and communications capabilities	6 - Wingman Principle 3 - Consequences of breeches



Question Number	Question	Subcategory
12	A potential motive for exploiting USAF cyberspace systems is to gather intelligence or commit espionage	7 - Wingman Principle 3 - Motives for Exploitation
13	A potential motive for exploiting USAF cyberspace systems is to conduct counter narcotic operations	7 - Wingman Principle 3 - Motives for Exploitation
14	A potential motive for exploiting USAF cyberspace systems is to access intellectual property	7 - Wingman Principle 3 - Motives for Exploitation
15	A potential motive for exploiting USAF cyberspace systems is to disrupt USAF systems or operations	7 - Wingman Principle 3 - Motives for Exploitation
29	An adversary can gain valuable information from information you post on social media, like Facebook or Twitter	8 - Wingman Principle 4 - At Work and Home
35	You are allowed to use a thumbdrive to transfer information from a USAF computer to your home computer	8 - Wingman Principle 4 - At Work and Home
36	You are allowed to burn information to a CD to transfer information from a USAF computer to your home computer	8 - Wingman Principle 4 - At Work and Home
25	Your gender is considered Personally Identifiable Information (PII) and should be protected	9 - Wingman Principle 5 & 6 - Personally Identifiable Information
26	Your military rank is considered Personally Identifiable Information (PII) and should be protected	9 - Wingman Principle 5 & 6 - Personally Identifiable Information
27	Your job description is considered Personally Identifiable Information (PII) and should be protected	9 - Wingman Principle 5 & 6 - Personally Identifiable Information
28	Your cellular phone number is considered Personally Identifiable Information (PII) and should be protected	9 - Wingman Principle 5 & 6 - Personally Identifiable Information
31	On a USAF network, it is acceptable to open an attachment from someone you do not know as long as you run it through a virus scanner prior to opening it	10 - Wingman Principle 7
34	You should never click on a link in an e-mail unless the e-mail is digitally signed or you can directly verify the source	10 - Wingman Principle 7
33	It is acceptable to download games listed on a USAF network as long as they are on the USAF 'Approved Gaming' list	11 - Wingman Principle 8
37	You are allowed to use Social Media, such as Facebook or Twitter, on a USAF network	11 - Wingman Principle 8
30	If you see classified information on a public website, it is acceptable to download it because once information is posted on a public site it is no longer classified	12 - Wingman Principle 9
32	You can install free Department of Defense anti-virus software on your home computer	13 - Wingman Principle 10

## Appendix E – Likert Summation and Average

Question Number	Question	Subcategory	Summation (33 - 165)	Mean
1	USAF uses cyberspace for conducting fire protection	1 - AF Use of Cyberspace	97*	3.13
2	USAF uses cyberspace for vehicle maintenance control	1 - AF Use of Cyberspace	118	3.58
3	USAF uses cyberspace for operating remotely piloted aircraft (RPA)	1 - AF Use of Cyberspace	151	4.58
4	USAF uses cyberspace for sending e-mails/surfing web	1 - AF Use of Cyberspace	156	4.73
5	USAF uses cyberspace for conducting intelligence, surveillance and reconnaissance operations	1 - AF Use of Cyberspace	157	4.76
6	A cyberspace vulnerability is a weakness in an information system or system security procedures that can be exploited	2 - Key Terms	148	4.48
16	A cyberspace vulnerability is a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of the occurrence	2 - Key Terms	131	3.97
18	Social engineering is an attempt to trick someone into revealing information that they would not normally reveal	2 - Key Terms	121	3.97
22	Cyberspace security principles apply when operating your smart phone	3 - Wingman Principle 1 - ID cyberspace systems	138	4.18
23	Cyberspace security principles apply when operating on a USAF network	3 - Wingman Principle 1 - ID cyberspace systems	156	4.73
24	Cyberspace security principles apply when operating on your home computer or private network	3 - Wingman Principle 1 - ID cyberspace systems	135	4.09
7	Employees are a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace	136	4.12
8	Criminal organizations are a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace	153	4.64
9	Individuals or small groups are a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace	141	4.27
10	The National Security Agency (NSA) is a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace	91	2.76
11	The Federal Bureau of Investigation (FBI) is a potential threat to USAF cyberspace operations	4 - Wingman Principle 1 - Threats to AF Cyberspace	89	2.7
17	Planting malicious code, worms, or botnets in common websites, software, or hardware is one method for exploiting USAF networks	5 - Wingman Principle 2	148	4.48
19	Failure to secure USAF cyberspace systems could result in adversaries gaining information about USAF current and future operational plans	6 - Wingman Principle 3 - Consequences of breeches	152	4.61
20	Failure to secure USAF cyberspace systems could result in the loss of USAF technological advantages	6 - Wingman Principle 3 - Consequences of breeches	147	4.45
21	Failure to secure USAF cyberspace systems could result in the loss of command, control, and communications capabilities	6 - Wingman Principle 3 - Consequences of breeches	154	4.67

\* Two surveys did not contain a response to this question. As a result, the scale for this particular question is (31-155).

Question Number	Question	Subcategory	Summation (33 - 165)	Mean
12	A potential motive for exploiting USAF cyberspace systems is to gather intelligence or commit espionage	7 - Wingman Principle 3 - Motives for Exploitation	137	4.15
13	A potential motive for exploiting USAF cyberspace systems is to conduct counter narcotic operations	7 - Wingman Principle 3 - Motives for Exploitation	112	3.39
14	A potential motive for exploiting USAF cyberspace systems is to access intellectual property	7 - Wingman Principle 3 - Motives for Exploitation	139	4.21
15	A potential motive for exploiting USAF cyberspace systems is to disrupt USAF systems or operations	7 - Wingman Principle 3 - Motives for Exploitation	142	4.3
29	An adversary can gain valuable information from information you post on social media, like Facebook or Twitter	8 - Wingman Principle 4 - At Work and Home	149	4.52
35	You are allowed to use a thumbdrive to transfer information from a USAF computer to your home computer	8 - Wingman Principle 4 - At Work and Home	49	1.48
36	You are allowed to burn information to a CD to transfer information from a USAF computer to your home computer	8 - Wingman Principle 4 - At Work and Home	58	1.76
25	Your gender is considered Personally Identifiable Information (PII) and should be protected	9 - Wingman Principle 5 & 6 - Personally Identifiable Info	106	3.21
26	Your military rank is considered Personally Identifiable Information (PII) and should be protected	9 - Wingman Principle 5 & 6 - Personally Identifiable Info	125	3.79
27	Your job description is considered Personally Identifiable Information (PII) and should be protected	9 - Wingman Principle 5 & 6 - Personally Identifiable Info	139	4.21
28	Your cellular phone number is considered Personally Identifiable Information (PII) and should be protected	9 - Wingman Principle 5 & 6 - Personally Identifiable Info	138	4.18
31	On a USAF network, it is acceptable to open an attachment from someone you do not know as long as you run it through a virus scanner prior to opening it	10 - Wingman Principle 7	61	1.85
34	You should never click on a link in an e-mail unless the e-mail is digitally signed or you can directly verify the source	10 - Wingman Principle 7	146	4.42
33	It is acceptable to download games listed on a USAF network as long as they are on the USAF 'Approved Gaming' list	11 - Wingman Principle 8	90	2.73
37	You are allowed to use Social Media, such as Facebook or Twitter, on a USAF network	11 - Wingman Principle 8	114	3.45
30	If you see classified information on a public website, it is acceptable to download it because once information is posted on a public site it is no longer classified	12 - Wingman Principle 9	63	1.91
32	You can install free Department of Defense anti-virus software on your home computer	13 - Wingman Principle 10	112	3.39

### Appendix F – Likert Responses Per Rating

Question Number	Strongly Disagree	Disagree	Neither Agree or Disagree	Agree	Strongly Agree
1	3	4	13	8	3
2	1	3	10	14	5
3	0	1	2	7	23
4	0	0	3	3	27
5	0	0	2	4	27
6	1	0	3	7	22
16	0	2	10	8	13
18	1	2	12	10	8
22	1	0	6	11	15
23	0	0	1	7	25
24	0	2	4	16	11
7	1	0	8	9	15
8	0	0	0	12	21
9	1	1	1	15	15
10	7	4	14	6	2
11	7	6	12	6	2
17	0	0	4	9	20
19	0	0	1	11	21
20	0	1	4	7	21
21	0	0	1	9	23
12	1	2	5	8	17
13	2	2	16	7	6
14	1	0	6	10	16
15	2	1	3	6	21
29	2	0	1	6	24
35	23	6	3	0	1
36	18	7	6	2	0
25	5	5	8	8	7
26	2	5	2	13	11
27	1	2	1	14	15
28	1	2	4	9	17
31	20	4	5	2	2
34	1	1	2	8	21
33	7	2	18	5	1
37	3	1	13	10	6
30	18	7	4	1	3
32	5	2	11	5	10

## Bibliography

- [1] Secretary of the Air Force Michael Wynne and Chief of Staff General Norton Schwartz. *Letter to Airmen*. 7 December 2005  
<http://www.24af.af.mil/shared/media/document/AFD-111003-050.pdf>  
(accessed 26 April 2012).
- [2] Secretary of the Air Force Michael Wynne and Chief of Staff General Norton Schwartz. *Letter to Airmen*. 7 May 2007.  
<http://www.af.mil/news/story.asp?id=123052273> (accessed 4 April 2012).
- [3] *Rise of the Cyber Wingman*. Staff Report Secretary of the Air Force Public Affairs 12 November 2009. <http://www.af.mil/news/story.asp?id=123177473> (accessed 27 April 2012).
- [4] Department of the Air Force. *Total Force Development*. AFI 36-26. Washington: HQ USAF, 27 September 2011. <http://www.e-publishing.af.mil/shared/media/epubs/AFPD%2036-26.pdf> (accessed 37 April 2012).
- [5] Wabiszewski, Michael G., SMSgt USAF. "BMT Accessions Lesson Dates," Electronic Message 0923 EST, 2 February 2012.
- [6] Air Force Cyberspace Technical Center of Excellence.  
<http://www.afit.edu/en/CCR/centerinfo.cfm?a=about> (accessed 30 April 2012).
- [7] Department of the Air Force. *Policy Guidance Memorandum on Ancillary Training*. AFI 36-2201V1\_AFGM2. HQ USAF/A1, 26 March 2009.
- [8] "The Book 2011," *Airman Magazine*, vol. LV, no. 3. (12 April 2012).  
<http://airman.dodlive.mil/book-archives/the-book-2011/> (accessed 25 May 2012).
- [9] Boleng, Jeff Lt Col USAF, Dr. Dennis Schweitzer, David S. Gibson Col USAF, "Developing Cyber Warriors". US Air Force Academy, CO  
<http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/boleng2008a.pdf> (accessed 1 May 2012).

- [10] Edwards, David. "Cadets Study Art of Cyber Warfare" 20 July 2011. <http://www.usafa.af.mil/news/story.asp?id=123264622> (accessed 1 May 2012).
- [11] U.S. Air Force ROTC Website <http://afrotc.com/college-life/courses/descriptions/> (accessed 25 May 2012).
- [12] United States Air Force Holm Center, "Cyberspace Lesson Plan," Maxwell AFB, AL 2012.
- [13] Lindsey, Shawn. "AFROTC To Host Cyber Warfare Speaker" 15 February 2010. <http://www.uh.edu/news-events/stories/2010articles/Feb2010/CyberWarfare.php> (accessed 1 May 2012).
- [14] Guerin, David "Louisiana Tech ROTC commander wins national award," 1 April 2008. [http://www.eurekalert.org/pub\\_releases/2008-04/ltu-ltr040108.php](http://www.eurekalert.org/pub_releases/2008-04/ltu-ltr040108.php) (accessed 1 May 2012).
- [15] Officer Training School Factsheet. 24 November 2010. <http://www.af.mil/information/factsheets/factsheet.asp?id=4703> (accessed 1 May 2012).
- [16] Holm Center Syllabus MMOPM-BOT-MOTS-001. "Basic Officer Training" September 2010. [http://www.afoats.af.mil/OTS/documents/BOT\\_Syllabus\\_AY\\_10\\_11.pdf](http://www.afoats.af.mil/OTS/documents/BOT_Syllabus_AY_10_11.pdf) (accessed 3 May 2012).
- [17] Department of the Air Force. *Information For Designers of Instructional Systems – ISD Executive Summary For Commanders and Managers*. AFH 36-2235 Volume 1. Washington: HQ USAF, 2 September 2002. <http://www.e-publishing.af.mil/shared/media/epubs/AFH36-2235V1.pdf> (accessed 2 May 2012).
- [18] Department of the Air Force. *Information for Designers of Instructional Systems For Basic Military Training*. AFH 36-2235 Volume 13. Washington: HQ USAF, 6 August 2003. <http://www.e-publishing.af.mil/shared/media/epubs/AFH36-2235V13.pdf> (accessed 2 May 2012).
- [19] Air Education and Training Command. *Technical and Basic Military Training Development*. AETCI36-2203\_AETGM2. Texas: Randolph AFB, 18 May 2012. <http://www.e-publishing.af.mil/shared/media/epubs/AETCI36-2203.pdf> (accessed 30 April 2012).

- [20] Wisher, Robert A. and J. Dexter Fletcher. "The Case for Advanced Distributed Learning" *Information and Security* vol 14, 2004. [http://infosec.procon.bg/contents/vol\\_14.htm](http://infosec.procon.bg/contents/vol_14.htm) (accessed 2 May 2012).
- [21] Molenda, Michael. "In Search of the Elusive ADDIE Model" *Performance Improvement* May/June 2003. <http://www.comp.dit.ie/dgordon/Courses/ILT/ILT0004/InSearchofElusiveADDIE.pdf> (accessed 5 May 2012).
- [22] Bates, Reid. "A critical analysis of evaluation practice: the Kirkpatrick model and the principle of beneficence" *Evaluation and Program Planning*, 27: 341-341(2007). [http://aetcnec.ucsf.edu/evaluation/bates\\_kirkp\\_critique.pdf](http://aetcnec.ucsf.edu/evaluation/bates_kirkp_critique.pdf) (accessed 12 May 2012).
- [23] Kirkpatrick, Jim PhD and Wendy Kayser Kirkpatrick. "The Kirkpatrick Four Levels: A Fresh Look After 50 Years 1959 - 2009," April 2009. <http://www.kirkpatrickpartners.com/LinkClick.aspx?fileticket=jI-C-94JMME%3d&tabid=56&mid=442> (accessed 5 May 2012).
- [24] AirForce.com. <http://www.airforce.com/joining-the-air-force/enlisted-overview/> (accessed 5 May 2012).
- [25] Department of the Air Force. "Officer Qualifying Test Information Pamphlet" AFPT 997. [http://www.airforce.com/pdf/AFOQT\\_S\\_Pamphlet\\_REV.pdf](http://www.airforce.com/pdf/AFOQT_S_Pamphlet_REV.pdf) (accessed 5 May 2012).
- [26] Air Force Personnel Center Website. 29 February 2012. <http://www.afpc.af.mil/library/airforcepersonnel demographics.asp> (accessed 5 May 2012).
- [27] United States Air Force Academy Website. [http://www.academyadmissions.com/#Page/Student\\_Eligibility](http://www.academyadmissions.com/#Page/Student_Eligibility) (accessed 5 May 2012).
- [28] Zickuhr, Kathryn. "Generations and Their Gadgets" *Pew Internet & American Life Project*. 3 February 2011. <http://pewinternet.org/Reports/2011/Generations-and-gadgets.aspx> (accessed 5 May 2012).
- [29] Air Education and Training Command. *Technical and Basic Military Training Evaluation*. AETCI 36-2201. Texas: Randolph AFB. 13 September 2010. <http://www.e-publishing.af.mil/shared/media/epubs/AETCI36-2201.pdf> (accessed 5 May 2012).

- [30] Department of the Air Force. *Air Force Training Program*. AFI 36-2201. 15 September 2010. <http://www.e-publishing.af.mil/shared/media/epubs/AFI36-2201.pdf> (accessed 5 May 2012).
- [31] AETC/A3T. "Request Review of 'Cyberspace and the Air Force' Curriculum" Electronic Message, 6 March 2012.
- [32] Johns, Rob. "Likert Items and Scales" Survey Question Bank: Methods Fact Sheet 1. March 2010. <http://www.surveynet.ac.uk/sqb/datacollection/likertfactsheet.pdf> (accessed 7 May 2012).
- [33] Department of the Air Force. *Guidebook For Air Force Instructors*. AFM 36-2236. Washington: HQ USAF, 12 November 2003. <http://www.e-publishing.af.mil/shared/media/epubs/AFMAN36-2236.pdf> (accessed 8 May 2012).
- [34] USAF BMT Plan of Instruction, *BlockII Unit 16 'Cyberspace and the Air Force' Change 1*, 22 November 2010.
- [35] Air Force Education and Training Course Announcement (ETCA) Website. <https://etca.randolph.af.mil> (accessed 3 May 2012).
- [36] Kirkpatrick, Jim, PhD and Wendy Kayser Kirkpatrick. *Training on Trial: How Workplace Learning Must Reinvent Itself to Remain Relevant*. New York: AMACOM, 2010. <http://www.kirkpatrickpartners.com/LinkClick.aspx?fileticket=zAcDCP6H2T4%3d&tabid=56&mid=415> (accessed 25 May 2012).



## Vita



# BIOGRAPHY



## UNITED STATES AIR FORCE

### MAJOR APRIL L. WIMMER

Major April L. Wimmer is a student at the Air Force Institute of Technology where she is completing her in-residence Intermediate Developmental Education. Upon completion of the program she will be awarded a Master of Science degree in Cyber Warfare.

Major Wimmer enlisted in the Air Force in 1993 as an aerospace propulsion apprentice. She received an appointment to the United States Air Force Academy Preparatory school under the Leaders Encouraging Airman Development program in 1995 and received her commission in 2000 through the United States Air Force Academy. She has developed operational expertise in the Minuteman III and MILSTAR weapon systems. She served as an ICBM mission ready instructor and emergency war order trainer, group and wing executive officer, and MILSTAR evaluator and branch chief. As Chief of Space Support Programs, she was responsible for 17 Program Elements worth of \$24.B during the development of the Air Force Space Command Program Objective Memorandum. Prior to her current assignment, Major Wimmer served as Legislative Liaison on the Headquarter's Air Force Space Command Commander's Action Group (CAG).



### EDUCATION

- 2000 Bachelor of Science in Space Operations, United States Air Force Academy, Colorado Springs, Colorado
- 2001 Top Graduate Officer Space Prerequisite Training, Vandenberg Air Force Base, California
- 2001 Distinguished Graduate ICBM Operations Training, Vandenberg Air Force Base, California
- 2004 Top Third Graduate Squadron Officer School, Maxwell Air Force Base, Alabama
- 2005 Master of Science in Space Studies, University of North Dakota, Grand Forks, North Dakota
- 2006 Academic Achievement Milstar Satellite Mission Control Subsystem Initial Qualification Training, Vandenberg Air Force Base, California
- 2007 National Security Space Institute Space 200
- 2009 Air Command and Staff College (correspondence)

*(Current as of May 2012)*



# BIOGRAPHY



## UNITED STATES AIR FORCE

### MAJOR APRIL L. WIMMER

#### ASSIGNMENTS

1. September 2000 – July 2001, Student Officer Space Prerequisite and ICBM Operations Training, 392nd Training Squadron, Vandenberg Air Force Base, California
2. July 2001 – July 2005, MMIII ICBM Missile Combat Crew Commander, Instructor Missile Combat Crew Commander, Assistant Current Operations Flight Commander, Wing Emergency War Orders Instructor, Group Executive Officer and Wing Executive Officer; 490th Missile Squadron, 341st Operations Support Squadron, 341st Operations Group, and 341st Space Wing, Malmstrom Air Force Base, Montana
3. July 2006 – Sept 2006, Student Milstar Satellite Mission Control Subsystem Initial Qualification Training, 533rd Training Squadron, Vandenberg Air Force Base, California
4. October 2006 – February 2009, Milstar Mission Commander, Evaluator, Chief Standardization Branch, and Chief Inspections Branch; 4th Space Operations Squadron and 50th Operations Group, Schriever Air Force Base, Colorado
5. February 2009 – January 2010, Chief, Space Support Programs; Directorate of Plans, Programs and Analyses, Headquarters Air Force Space Command, Peterson Air Force Base, Colorado
6. January 2010 – May 2011, Legislative Liaison, Commander's Action Group, Headquarters Air Force Space Command, Peterson Air Force Base, Colorado
7. May 2011 – Present, Student, Air Force Institute of Technology, Wright Patterson Air Force Base, Ohio

#### MAJOR AWARDS AND DECORATIONS

Meritorious Service Medal with one oak leaf cluster  
Air Force Commendation Medal  
Air Force Achievement Medal with one oak leaf cluster  
AF Outstanding Unit Award with four oak leaf clusters  
Combat Readiness Medal  
National Defense Service Medal with one device  
Global War on Terrorism Service Medal

#### EFFECTIVE DATES OF PROMOTION

Second Lieutenant	May 31, 2000
First Lieutenant	May 31, 2002
Captain	May 31, 2004
Major	January 1, 2010

*(Current as of May 2012)*

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 074-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p><b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b></p>					
1. REPORT DATE (DD-MM-YYYY) 14-06-2012		2. REPORT TYPE Graduate Research Project		3. DATES COVERED (From – To) May 2011 – June 2012	
4. TITLE AND SUBTITLE  Evaluating the Effectiveness of Air Force Foundational Cyberspace Training				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)  Wimmer, April L., Major, USAF				5d. PROJECT NUMBER N/A	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765				8. PERFORMING ORGANIZATION REPORT NUMBER  AFIT/ICW/ENG/12-05	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Cyberspace Technical Center of Excellence Attn: Dr. Harold J. Arata 2950 Hobson Way WPAFB, OH 45433-7765 <a href="mailto:harold.arata@afit.edu">harold.arata@afit.edu</a> (937) 255-3636 x7105; DSN 785-3636, x7106				10. SPONSOR/MONITOR'S ACRONYM(S) AF CyTCoE	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.					
13. SUPPLEMENTARY NOTES This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.					
14. ABSTRACT: Each Airman's actions on the network impact the ability to execute the broader Air Force mission. The Air Force instituted cyberspace training during initial training programs and introduced the "Cyber Wingman Philosophy" to guide Airmen's daily cyberspace conduct. This paper examines the effectiveness of cyberspace training established for all Active Duty Air Force officer and enlisted members. Specifically, it summarizes current training, reviews the mechanisms established to evaluate the effectiveness of that training, and determines if current training programs are meeting the desired training goals. The research uses a twofold approach. First, it applies inductive research to analyze the existing training and evaluation mechanisms. Second, it includes a survey mechanism to model the attitudes of individuals who have received training. The research concludes that the next step in Air Force cyberspace training is to determine the effectiveness of the training. Analysis revealed the need to establish clearly defined objectives for Air Force Foundational Cyberspace Training; complete a pre-post attitude assessment survey; and inclusion of curriculum developers in the process and feedback to both curriculum developers and cyberspace users is crucial. Cyberspace is critical to Air Force operations and the quality of the training should mirrors the importance of the mission.					
15. SUBJECT TERMS Cyberspace Training, Cyberspace and the Air Force					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jonathan W. Butts, Major, USAF, PhD (ENG)
U	U	U	UU	75	19b. TELEPHONE NUMBER (Include area code) (937) 257-3636 x4332; jonathan.butts@afit.edu