COURSE CURRICULUM DEVELOPMENT FOR THE FUTURE CYBERWARRIOR

GRADUATE RESEARCH PROJECT

Mark A. Chacon, Major, USAF

AFIT/IC4/ENG/06-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/IC4/ENG/06-02

COURSE CURRICULUM DEVELOPMENT FOR THE FUTURE CYBER WARRIOR

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical & 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 C4I Systems

Mark A. Chacon, BBA, MS

Major, USAF

June 2006

AFIT/IC4/ENG/06-02

COURSE CURRICULUM DEVELOPMENT FOR THE FUTURE CYBER WARRIOR

Mark A. Chacon, BBA, MS

Major, USAF

Approved:

//Signed//	9 Jun 06
Robert F. Mills, PhD, USAF (Chairman)	Date
//Signed//	9 Jun 06
Michael R. Grimaila, PhD, USAF (Member)	Date

To my Mother and Father who always stressed that education was the key…

Acknowledgments

I would like to express my sincere appreciation to my advisors and mentors, Dr. Bob Mills and Dr. Mike Grimaila for their guidance and support throughout the course of this research effort, and throughout my academic tenure at AFIT. I would also like to thank the members of my class for the camaraderie we shared together through thick and thin, from the IDEF and STATS marathon sessions, to the friendly competition on the walleyball court—truly these are the memories I'll cherish most. Finally, and most importantly, I'd like to thank God for giving me the strength, perseverance, friends, and loved ones to get me through one of the most difficult periods of my life.

Mark A. Chacon

Abstract

Cyberspace is one of the latest buzzwords to gain widespread fame and acceptance throughout the world. One can hear the term being used by presidents of states to elementary children delving into computers for the first time. Cyberspace has generated great enthusiasm over the opportunities and possibilities for furthering mankind's knowledge, communication, as well as, creating more convenient methods for accomplishing mundane or tedious tasks. But for all the good that cyberspace has created, it has a dark side also.

This dark side manifests itself in the form of malicious individuals, organizations, and nations who have learned, or are learning, to exploit the weaknesses within cyberspace itself. These malicious entities then use cyberspace as a weapon against the very countries that rely on it most. This use of cyberspace has created a "fourth dimension" (the second and third, being ground and air/space forces) in warfare where the enemy may be completely unseen, or unknown, but no less of a threat. Without a doubt, cyber warfare has become the poor man's method to anonymously strike back at sovereign countries without declaring hostilities or facing troops on the battlefield.

In order to thwart the efforts of the "enemy" entities, cyberspace reliant countries have/are beginning to educate and train themselves in the art of fourth dimensional warfare, but the learning curve is steep. In many cases, experts have a hard time agreeing on what assets should be included in the cyberspace realm. This paper will attempt to define the emerging thoughts on cyberspace and cyber warfare, and relate them into a

course curriculum that can best prepare the IDE field grade officer to face the challenges on the cyber frontlines.

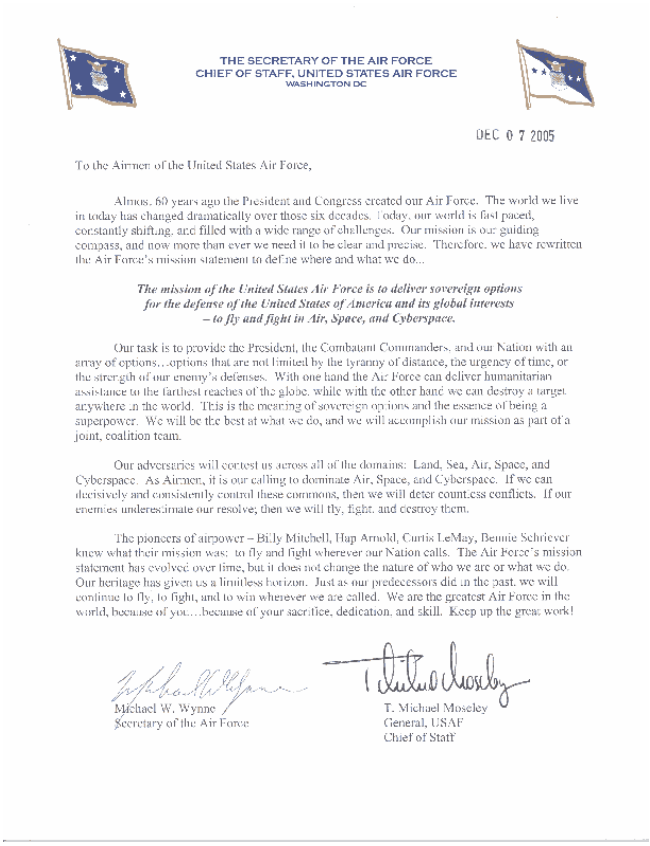
Table of Contents

List of Figures

COURSE CURRICULUM DEVELOPMENT FOR THE FUTURE CYBERWARRIOR

Introduction

On 7 December 2005, Michael Wynn, the Secretary of the Air Force, and T. Michael Moseley, the Chief of Staff of the Air Force, jointly issued a new mission statement for the United States Air Force. "The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and it global interests—to fly and fight in the Air, Space and *Cyberspace*."[1] (Figure 1) With these words, the SECAF and CSAF made it abundantly clear that cyberspace is officially part of the battlespace in which airmen will be operating.



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

DEC 0 7 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 President, 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, Bennie 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

Figure 1—Letter to Airmen, 7 Dec 2005

Cyber related activities, such as, information operations, information warfare, network warfare, etc., are not new

[1] Michael Wynn and T. Michael Mosely, Letter to the Airmen of United States Air Force, 7 Dec 2005

concepts to airmen who been part of the service since the mid-1990s. What is new is the 2005 mission statement acknowledges cyberspace as a domain where defensive, as well as, offensive operations would take place. Prior to this mission statement, computer network warfare was mostly focused on defensive operations.[2]

The 2005 mission statement is a bold and visionary step toward expanding Air Force capabilities and proficiencies, but it also creates a conundrum for the warfighter. This conundrum comes in the form of multiple questions. What exactly is cyberspace? Who or what is a threat to our nation in cyberspace? What warfighting assets will operate in the cyberspace, and how will we properly choose the people to "organize, train, and equip" for this new medium?

[2] Maj Scott D. Tobin, *Establishing a Cyber Warrior Force*, AFIT Thesis, Sep 2004

Cyberspace, the Final Frontier?

"Peace really does not exist in the Information Age."

Lt Gen Kenneth Minihan, USAF
Director, NSA
4 June 1998

William Gibson is credited with coining the term cyberspace in 1984 with this book entitled Neuromancer. In his book, he defines cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding…"[3] While Mr. Gibson's description is a grandiose vision of cyberspace, Whatis.com has a more succinct definition. "Cyberspace is the total interconnectedness of human beings through computers and telecommunication without regard to physical geography."[4]

So what does this mean to the Air Force? Our mission statement clearly states that we'll fight in the cyberspace domain, but yet most people still will question what exactly is cyberspace. This is one of the most difficult and perplexing questions to answer, because there are so many differing opinions. "Cyberspace is more of a metaphor than a precise concept, and it has different meanings in different contexts."[5] At the time of this writing, the Air Force has not developed a clear, concise definition of

---

[3] William Gibson, *Neuromancer*, Penguin Group, 1984.
[4] http://www.whatis.com

what it perceives cyberspace to be, and what is included. Because of this, the Air Force has created a cyberspace task force under the direction of Dr Lani Kass to make sense of this puzzle, and to ensure all future AF cyber warriors are working off the same sheet of music.

Why does the warfighter care about cyberspace and what is encompassed by it? At the simplest level, cyberspace includes almost every portion of electronic (and now light) communications and information spectrum. Therefore any technology that is connected and communicating through cyberspace will affect the warfighters ability to effectively execute their mission. As the old saying goes "no Comm, no bomb." This means that everyone from a casual user surfing the internet, to a

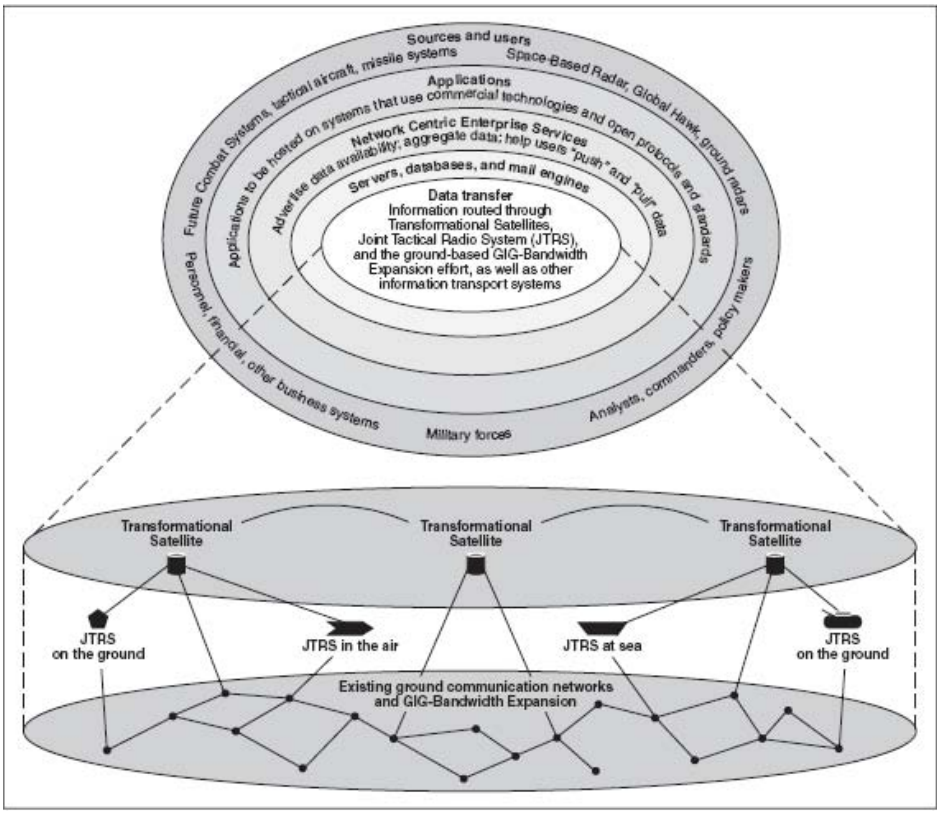


Figure 2—Source: GAO-04-858, The Global Information Grid and Challenges Facing its Implementation

---

[5] Eric A. Fisher, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options,*

fighter aircraft receiving targeting information via a Link-16 circuit, are operating in and affected by what happens in cyberspace. Furthermore, as the Air Force, and other branches, slowly transition to the Global Information Grid (GIG) (See Figure 2) cyberspace will become even more of a factor to users on every level of the battlefront. The 2006 Quadrennial Defense Review Report describes the GIG as "a globally interconnected, end-to-end set of trusted and protected information networks. The GIG optimizes the processes for collecting, processing, storing, disseminating, managing and sharing information with in the Department [of Defense] and with other partners."[6] Being able to achieve "cyber-supremacy" on this battlefront, will be no different than air supremacy or space supremacy in the physical world.

Unfortunately, this thought process also carries the associated biases and cultural stereotypes inherent with the military environment. When discussing the far-reaching effects of cyberspace operations with one of my operator colleagues, he commented that it sounded like "everything is part of cyberspace, and that the communications people are empire building." This is where I disagree with him. Even though cyberspace uses the connectivity normally associated with communications professionals, cyberspace belongs to all the operators who use it to accomplish their warfighting goals. Suffice it to say, that cyberspace is going to be a tough nut to crack, and the Air Force will have to shift its cultural paradigms to effectively harness it.

Congressional Research Service RL 32777, The Library of Congress, 22 Feb 2005.
[6] Department of Defense, Quadrennial Defense Review Report, 6 Feb 2006

Who/What is the Threat?

"In the past you would count the number of bombers and the number of tanks your enemy had. In the case of cyberwar, you really can't tell whether the enemy has good weapons until the enemy uses them."

Richard Clarke,
Former Director of Cybersecurity for the White House

Some people believe that the threats of cyberwarfare, cyberterrorism, cybercrime, and the like, are the makings for good science fiction writing. They scoff at the idea that a group of individuals with cyber technology (e.g. computers) could do any discernable damage to a powerful nation. Is this view correct? To answer this question one would have properly discern the category and nature of the threat.

Some of the broad categories that a cyberspace threat can manifest itself are: hacker activities, criminal acts (both insider and outsider), terrorism, and/or nation-state actions. Because of this broad range of categories, operators in cyberspace must always be on their guard, defending the fourth dimension. "According to an August 2005 computer security report by IBM, more than 237 million overall security attacks were reported globally during the first half of the year. Government agencies were targeted the most, reporting than 54 million attacks, while manufacturing ranked second with 36 million attacks, financial services ranked third with approximately 34 million, and healthcare received more than 17 million attacks."[7] This begs the question, out of all of these millions of attacks, how can we be sure which of the four categories they fall into? How do we know that the attack might not be a combination of two or more of the

[7] John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, Congressional Research Service RL 33123, The Library of Congress, 20 Oct 2005.

categories? The answer to this question is that often we can suspect, but we really can't be sure.

Hackers

In the first category, we have the hacker committing his/her attacks for personal prestige (or notoriety), knowledge, or genuine good intentions. A current high profile hacker case is that of a British citizen, Gary McKinnon. (Figure 3) Mr. McKinnon is facing possible extradition to the United States for hacking multiple DoD computer systems over a two period. He claimed his reason for breaking into the systems was to search for facts proving the United States government was withholding UFO technology information from the public.[8] To many, this may seem like another case of a normally law-abiding individual stupidly getting involved in the hacking game. What muddies the waters is the timing of his infiltrations. One of his most destructive attacks came shortly after the September 11, 2001 attacks on the World Trade Center and Pentagon. In this situation, his unauthorized intrusion resulted in a 300 computer network at a naval weapons station

Figure 3—Gary McKinnon, Source: www.bbc.com

[8] "UK Hacker Should be Extradited," BBC News, (10 May 2006); available from http://news.bbc.co.uk/2/hi/technology/4757375; accessed 15 May 2006.

being shut down for a week.[9] Should Gary McKinnon's actions place him in a hacker status, criminal trespasser status, or as a cyber terrorist who should be locked up at Gitmo with the rest of the detainees? Herein lays one of the biggest difficulties with operating in cyberspace—the lines are often too fuzzy and undefined.

Criminals

From the criminal category comes a 2004 case, where organized cybercriminals broke into the London office computer systems of the Japanese bank Sumitomo. Their intent was to steal 220 million British Pounds by transferring the money to other banks around the world.[10] Anybody reading this case would readily say that this action was a crime with the intent of making a quick buck at the bank's expense. But can we be so sure? How do we know that the true intent wasn't to help finance terrorist organizations around the world? Increasingly there are rumors of organizations procuring hacker services as cyberspace hired guns. "Other groups may be motivated by profit, or linked to organized crime, and may be willing to sell their computer skills to a sponsor, such as a nation state or a terrorist group, regardless of the political interests involved."[11] Once again, we are left wondering if we made the right assumptions about this group of people.

Terrorists

The third threat category is that of terrorists looking for new (and maybe less risky) ways to further their cause against their enemy. In the past, many western citizens

---

[9] US Army Training and Doctrine Command, DCSINT Handbook No. 1.02, *Cyber Operations and Cyber Terrorism*, 15 Aug 2005.
[10] John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, RL 33123, Congressional Research Service, The Library of Congress, 20 Oct 2005.
[11] Clay Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, RL32114, Congressional Research Service, The Library of Congress, 17 Oct 2003.

may have viewed terrorists as a backward group because of their low-tech guerilla tactics and their propensity for shunning anything viewed as a "western" idea. Because of this, it was believed that terrorists were somewhat mindless automatons who did their master's bidding without placing any thought into their actions. Events since that time have shown us otherwise. Although many terrorist groups still view the western lifestyle as decadent, they are quick to use the knowledge, conveniences, opportunities, and openness offered by our societies against us. "When U.S. troops recovered al Qaeda laptops in Afghanistan, officials were surprised to find its members more technologically adept than previously believed. They discovered structural and engineering software, electronic models of a dam, and information on computerized water systems, nuclear power plants, and U.S. and European stadiums."[12] Many cyber terrorism critics state that terrorists are using cyberspace for intelligence collection, physical attack coordination, and monetary transactions, and there are no reports or evidence of actual cyber terrorism against the United States. However, western governments can't be so callous to believe that this is a trend that won't change over time. Imam Samudra (Figure 4), a terrorist convicted for the 2002 bombings of two Bali nightclubs, wrote a book from his death row cell. In his book, he calls for Muslim youth to specifically refine their

Figure 4--Imam Samudra, Source: www.washingtonpost.com

hacking skills so they can attack U.S. computer networks.[13] Additionally, in the closing paragraphs of Gabriel Weimann's cyberterrorism report he makes a statement that needs to be heeded by information technology reliant countries throughout the world. "Future terrorists may indeed see greater potential for cyber terrorism than do terrorists of today…the next generation of terrorist is now growing up in a digital world, one in which hacking tools are sure to become more powerful, simpler to use, and easier to access. Cyber terrorism may also become more attractive as the real and virtual worlds become more closely coupled."[14]

Nation-State Actors

The final threat category this paper will focus on is that of nation-state actors. Of all the categories previously mentioned, this is potentially the most dangerous to the United States. The primary reasons are; nation-state actors have the proper financial resources, and usually, educational systems to support cyberspace exploration and exploitation. Furthermore, several of these nations believe a future conflict with the United States is inevitable. Because the U.S. has shown significant prowess on the battlefield, the opposing nations will look for an equalizer. To many, this equalizer comes in the form of our reliance on networks and cyberspace—our "Achilles' heel". "In testimony to the Senate Intelligence Committee in February 2005 the FBI Director noted, "The greatest cyber threat is posed by countries that continue to openly conduct computer

---

[12] Gabriel Weimann, *Cyberterrorism How Real Is the Threat?*, United States Institute of Peace, Special Report 119, December 2004.
[13] John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, RL 33123, Congressional Research Service, The Library of Congress, 20 Oct 2005
[14] Gabriel Weimann, *Cyberterrorism How Real Is the Threat?*, United States Institute of Peace, Special Report 119, December 2004.

network attacks and exploitations on American systems." "State actors have the technical and financial resources to support advanced network exploitation and attack."[15]

Our current global adversaries have also latched onto the concept that it easier to fight the U.S. from the shadows. The anonymity that cyberspace provides allows them to attack us on all levels simultaneously. Inversely, this same anonymity makes it difficult for the U.S. to retaliate in kind, for fear of causing collateral damage to allied and neutral nations. "Under the law of armed conflict, the use of force—and all out cyberwar is likely a "use of force"—must follow particular patterns. A warrior may not deliberately target non-combatants for attack. The use of force must be proportional to objectives, and reasonable effort must be taken to minimize collateral damage."[16] While the U.S. and it allies follow this convention, does it necessarily mean our adversaries will?

People's Liberation Army Colonels Qiao Liang and Wang Xiangsui demonstrated they understood the potential power of this type of attack when they wrote "if the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone

Figure 5—PRC Flag

---

[15] Thomas J. Barrett, *National Cyberguard; Defending America's Cyberspace against the Strategic Threat,* National Center at Norwich University-Applied Research Institute, 2005

[16] Mark Rasch, "Why the Dogs of Cyberwar stay leashed", SecurityFocus Online, 24 March 2003, accessed from www.theregister.co.uk.

communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty."[17] Colonel Liang's and Col Xiangsui's words proved to be prophetic when National Security Advisor, Condolessa Rice, made this statement in 2001. "Today the cyber economy is the economy. Corrupt those networks and you disrupt this nation"[18]

The previous examples demonstrate that the cyber threat is real on many different levels. It would be foolish for technology-reliant countries to believe otherwise. So where do we go from here? How do protect ourselves from these threats? And most importantly, what do we need to do to prepare our IDE cyberspace warriors of the future?

---

[17] Col Qiao Liang and Col Wang Xiangsui, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, China, February 1999.
[18] US Army Training and Doctrine Command, DCSINT Handbook No. 1.02, *Cyber Operations and Cyber Terrorism*, 15 Aug 2005.

The Future is Upon Us

As previously stated, the Air Force doesn't have an official definition of cyberspace, but this shouldn't stop warfighters from thinking of the potential capabilities it brings to the fight. When the airplane was first introduced into World War I operations, many short-sighted individuals viewed it only as an observation platform. By WWII the airplane had become an instrument of national will and policy.

I believe this is the point were at with cyberspace and cyber warfare. We recognize it is a relatively new medium, but we don't necessarily know how to effectively employ our forces. Cyberspace also carries the additional problem that there are no borders, (i.e., airspace, or territorial waters) associated with it, except for those erected by firewalls and intrusion detection systems. In other words, in the cyber world national sovereignty does not garner the same respect as it does in the physical world. As was previously seen in the Gary McKinnon hacking case, the United States cannot even lay claim (without British Parliament approval) to the intruder who ransacked our systems. If he had physically been caught infiltrating a base on U.S. soil, he would now be doing time in the SuperMax Federal prison with Zacarias Moussaoui. Finally, as pointed out previously, the use of weapons in cyberspace could prove to be just as detrimental to the attacker as it is to the defender.

As for a definition of cyberspace, the author will subscribe to the current cyberspace model proposed by Dr. Robert Mills and Dr. Richard Raines of the Air Force Institute of Technology that:

cyberspace = connectivity + content + cognition (see Figure 6)

In their model, connectivity refers to the physical ways cyberspace is interconnected, whether it be through landlines, wireless hubs, microwaves, satellite, etc. Content refers to the type of data, intelligence or information being transported through cyberspace (e.g. SIGINT, ELINT, HUMINT, etc). The cognition is the part where the human player takes the data/information/intelligence received through cyberspace and turns into knowledge to make decisions and plans to bend the enemy to our will.[19]

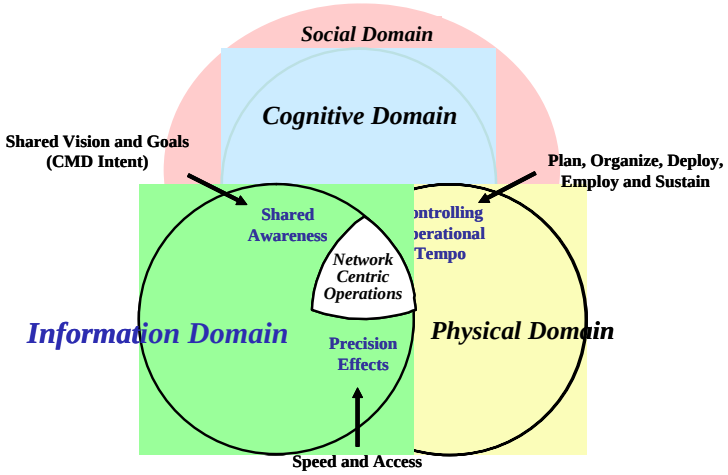


Figure 6—Producing IA, IO, and Cyber Warriors Briefing, 20 April 2006

The primary focus of cyberspace should be on the information that flows through it. Destruction, denial, and or deception of this information can paralyze, demoralize or panic an army. Several times during the American Civil War, the Army of the Potomac lost the initiative because they were under the false impression that Confederate forces were larger due to faulty information. To paraphrase Sun Tzu "the true pinnacle of military excellence is to subjugate the enemy without ever engaging them in combat." Cyberspace could be the perfect medium to practice this type of concept.

---

[19] Dr. Robert Mills and Dr Richard Raines, "Producing IA, IO, and Cyber warriors" briefing to BG Miller, 20 April 2006

Who's a Cyber Warrior?

Whether we know it or not, cyber warriors already exist in our world. "Unofficial" cyber warriors range from network system administrators, computer emergency response personnel, electronic warfare specialists, database administrators, telephone service providers, to the everyday computer user. The everyday computer user is a cyber warrior? How can this be possible?

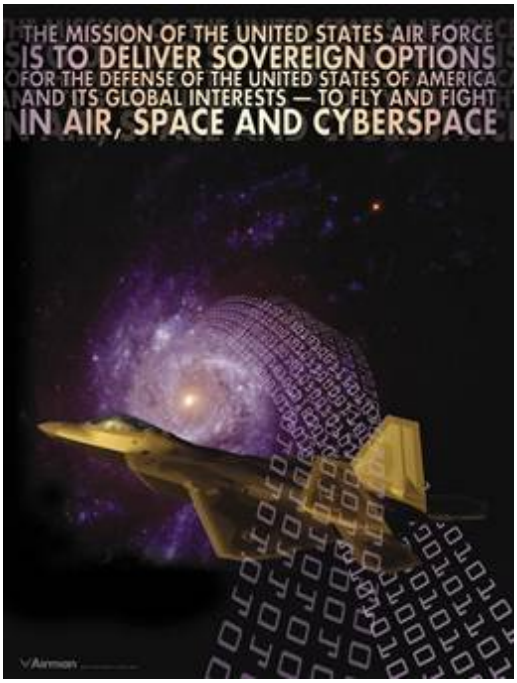


Figure 7—Cyberspace Mission

There is the old saying that "a chain is only as strong as its weakest link." The same goes for operating in cyberspace. If an ordinary user isn't following basic security practices, such as, good password naming conventions, locking their system when they step away from them, or recognizing social engineering attacks when they encounter them, they leave a way open for a potential intrusion and attack. The point being made here is that there isn't just one "elite" group of people who can and should be considered cyber warriors. "Users need to know the simple things that they can do to help to prevent intrusions, cyber attacks, or other security breaches. All users of cyberspace have some responsibility, not just for their own security but also for the overall security and health of cyberspace."[20]

---

[20] *The National Strategy to Secure Cyberspace*, February 2003.

Who Should become an "Official" Air Force Cyberwarrior?

Schools of Thought

This is a loaded question, and there seems to be two schools of thought on this subject. First you have the advocates who state that only an individual with a technical degree should be an "official" cyber warrior. In fact, one of my previous AFIT colleagues wrote in his thesis "Prior to their acceptance in the IO career force [cyber warfare], potential candidates should have a technical undergraduate degree. It's not essential that they complete an engineering or computer science degree, but it's important that their undergraduate program be technical in nature, and include several engineering or computer science courses. This technical undergraduate program will aid the individual in their completion of the initial IO [cyber warfare] course."[21]

I whole heartedly agree with Major Tobin's assessment that the degree will assist a person with this type of career field. But does this mean we turn away enlisted personnel who don't have the degree, but might have over 15 years of experience in networking along with all the certification? Wait a minute; we're talking about enlisted versus officers now. Are we sure there is a difference? What if the officer is a prior service person, who has years of experience in the communications/networking community, but decided to pursue an undergraduate degree in history? My point being that only using an undergraduate degree as a discriminator is not in the best interests of the Air Force. If the business world subscribed to this type of thinking, Bill Gates would

---

[21] Maj Scott D. Tobin, *Establishing a Cyber Warrior Force*, AFIT Thesis, Sep 2004

have never started Microsoft, and Michael Dell could have never started Dell Computers.

The other school of thought argues that only allowing "techno-geeks" in cyber operations field limits the effectiveness of the force. They argue that by allowing the engineers to dominate the career field, the stove-pipe views of cyberspace will persist. This is because there is an inherit belief that engineers are only interested in their particular field of study, and not necessarily the big operational picture. A 2005 Rand Report partially confirms this theory "Many young officers leave shortly after their initial obligation ends—an exodus that is attributed to the demand from the civilian sector. However, the civilian sector aside, it has also been argued that the career path for S&E [Science and Engineering] officers is generally not attractive. Unfortunately, most of the information on the latter issue is anecdotal…it was encouraged in the 1990s to assign anew S&E officer to an operational tour, not to an S&E position. Others argued that S&E officers are at their peak in subject-area currency when they graduate, and not using them in S&E positions wastes the Air Force's investment in their education, as well as disappointing them by separating them from the S&E world for two years."[22]

So who's wrong and who's right? In this case I would have to say both are. As in everything in life, there needs to be a good balance for optimal harmony. In this case we must put the question into the proper context. The question should be who in the Air Force needs (not should) attend the AFIT IDE cyber warfare course, and at what level should the course be taught? This is a different question all together. To properly assess the type of course to develop one has to closely look at the typical IDE select demographics and expectations.

IDE Demographics

First, AFIT IDE students are normally either mid-level or senior Majors who are coming from predominantly operations oriented career fields. Second, many of the

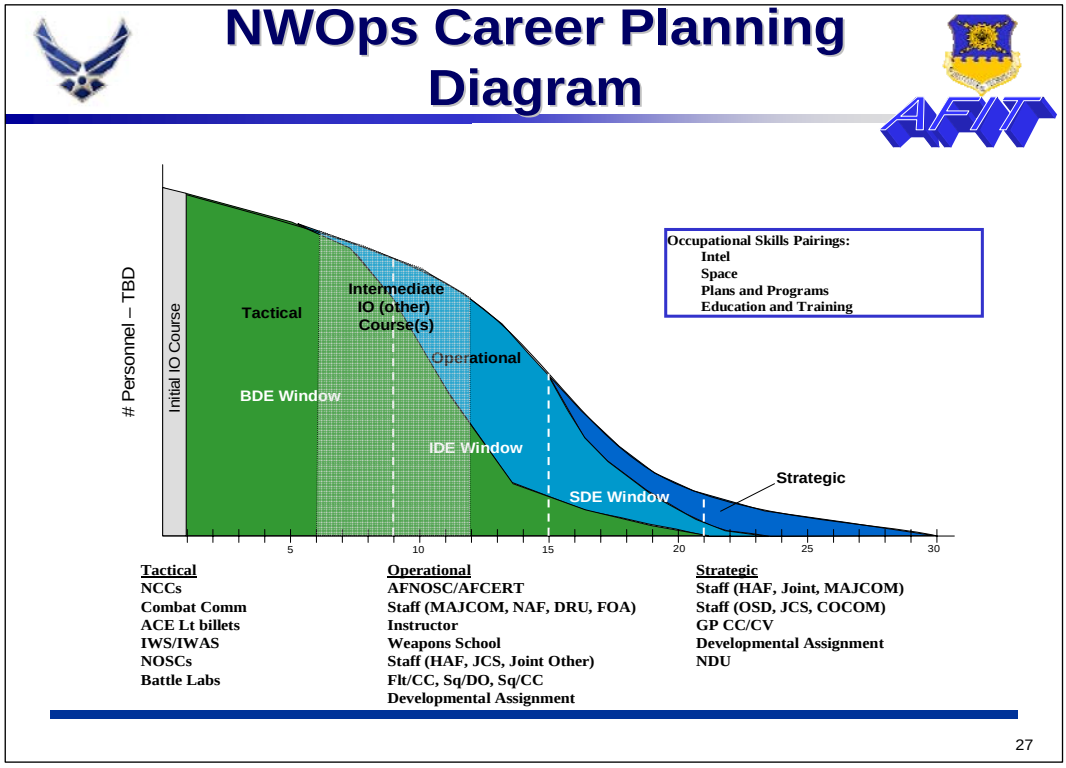


Figure 8—Source: Establishing A Cyber Warrior Force Thesis

Majors selected for IDE originally expected to attend Air Command and Staff College (or an equivalent military theory school) in residence and not necessarily working toward another master's degree. Finally, when these Majors leave AFIT they will be going to AIRSTAFF, MAJCOM, or similar type staff jobs—except for the fortunate few who get a command job. The point being is a majority will be going to what is predominantly looked at as "managerial" or "leadership" positions. In these cases, in-depth technical knowledge may be a plus, but not necessarily a must for the job. Instead the emphasis is

---

[22] Lionel Galway, Richard Buddin, Michael Thirtle, Peter Ellis, and Judith Mele, *Understrength Air Force*

placed on being a "big picture" thinker and seeing where cyberspace can fit into and support the strategic initiatives of the national command authority. Taking Major Tobin's "NWOps Career Planning Diagram" (see Figure 8) and correlating it to the demographics one can see how the word "cyber warrior" could easily be substituted for "NWOps".

Who Attends?

So who needs to attend the cyber warrior course? Without a doubt I would say anyone in a career field whose day to day job places them in a position where they have to make decisions regarding the use of cyberspace and its connecting equipment, or has to derive knowledge from information transmitted via cyberspace is a likely candidate.

The idea is to create a synergy where different AFSCs look at cyberspace with one common goal. The goal is to improve and exploit the timeliness, interoperability, resilience, and information of the medium in order to shorten the OODA loop and increase the lethality of the joint forces. "Therefore it is incumbent upon the command to organize the IO cell so that it has the necessary balance of talent and expertise to sort through the profusion of information available to the average military staff today."[23] This means upon course completion, a communications officer shouldn't have a blank stare because they don't know what LINK-16 is, how it works, or its importance to the flying community. The entire focus of the course would be to get people interacting about the strengths, weaknesses and possibilities in the cyberspace realm. They would receive broad thought provoking instruction on the issues facing cyber warriors, but not bury

---

Officer Career Fields, Rand Corporation, 2005.
[23] Leigh Armistead, *Information Operations*, Brassey's Inc., Washington D.C., 2004

them in the minutia of the technical details. To this effect, different educational backgrounds and operational experience can and will be brought to the table, ensuring groupthink and stovepiping does not become the norm. I think Dr Gossman and Mr Akita best describe the concept when they write "No matter how far technology advances, in the end it will be up to the individual, often working as part of a team, to understand the meaning of the information and to determine the best possible course of action given the potential grave consequences associated with military actions."[24]

Curriculum Development

Proper focus and development of the course is paramount. As stated previously, most IDE graduates will go on to be "big picture" thinkers at the operational level, so the course needs to be tailored toward this type of audience. The curriculum has to be current, thought provoking, and most important, relevant to the IDE cyber warrior. This is not to say that the IDE student shouldn't be exposed to some more technical concepts, but care needs to be taken to avoid taking them to a level where the information taught won't be useful. Chances are a senior IDE major graduate won't be coding logic bombs, or calculating the orbital mechanics of a satellite on their next job. These fundamental differences are the reason why the IDE technical program should and needs to be different from that of a "typical" AFIT master's accession.

Additionally, there have been multiple articles and research papers written that suggest more emphasis needs to be placed on the information and the processes surrounding the information, rather than the technology associate with it. In other words,

---

[24] Dr Jeff Grossman, and Richard Akita, "Global Threats Demand Credible Response in Less Time", Signal Magazine, March 2006.

the information, not necessarily the technology, should drive the car in the cyber realm. As Mr. Gilligan (former CIO of the Air Force) commented in his 3 April 2003 statement to the House Armed Services Committee "To guide our transformation and our investment decisions, we are specifying mission-oriented concepts of operations, or CONOPS, that define how we will conduct air and space operations with joint and coalition forces. A common characteristic across all these CONOPS is the need to provide the right information, at the right time to enable commanders to make the right decisions. This permits us to achieve "information dominance," that enables joint and coalition forces to prevail in any operational situation."[25] Unfortunately, it appears the services still have a way to go before they reach Mr Gilligan's idealized goal. In the 15 May 2006 issue of CIO Magazine, Allan Holmes reports "The GAO has charged that the Department of Defense's "substantial *long-standing management problems related to business operations* and systems have adversely affected the economy, efficiency and effectiveness of its operations; and, in some cases, impacted the morale of our fighting forces that are in harm's way."[26] This is precisely why the cyber warrior curriculum needs to be geared toward a combination of operational focus with some technical savvy. If the course focuses on only one the two, IDE graduates will not be properly armed with the knowledge needed to be operational big picture thinkers.

Finally, Joint Publication 3-13 for Information Operations clearly states why the United States needs to be dominant in the area of cyber warfare, and hence why a

---

[25] John Gilligan, Chief Information Officer United States Air Force Statement Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities House Armed Services Committee United States House of Representatives, 3 April 2003.
[26] Allan Holmes, "Federal IT Flunks Out", CIO Magazine, 15 May 2006.

balanced IDE course needs to be established at AFIT. ”History indicates that the speed and accuracy of information available to military commanders is the significant factor in determining the outcome on the battlefield. IO enables the accuracy and timeliness of information required by US military commanders by defending our systems from exploitation by adversaries. IO are used to deny adversaries access to their C2 information and other supporting automated infrastructures. Adversaries are increasingly exploring and testing IO actions as asymmetric warfare that can be used to thwart US military objectives that are heavily reliant on information systems. This requires the US military *to employ defensive technologies and utilize leading-edge tactics and procedures* to prevent our forces and systems from being successfully attacked.”[27]

[27] Joint Publication 3-13, *Information Operations*, 13 February 2006.

Proposed Curriculum for the Cyber Warrior IDE Course

Methodology

During the course of my research for this paper I explored other universities and institutes' programs related to cyber security, computer security, information assurance, and the like. Two things became very apparent. First, all of their courses were heavy on the technology, but light on the information and/or processes related to the information. Second, almost none focused on the impact of cyberspace to military operations.

INFORMATION OPERATIONS INTEGRATION INTO JOINT OPERATIONS (NOTIONAL)

Core, Supporting, Related Information Activities	Activities	Audience/ Target	Objective	Information Quality	Primary Planning/ Integration Process	Who does it?
Electronic Warfare	Electronic Attack	Physical, Informational	Destroy, Disrupt, Delay	Usability	Joint Operation Planning and Execution System (JOPES)/ Targeting Process	Individuals, Governments, Militaries
	Electronic Protection	Physical	Protect the Use of Electro-magnetic Spectrum	Security	JOPES/Defense Planning	Individuals, Businesses, Governments, Militaries
	Electronic Warfare Support	Physical	Identify and Locate Threats	Usability	Joint Intelligence Preparation of the Battlespace(JIPB)/SIGINT Collection	Militaries
Computer Network Operations	Computer Network Attack	Physical, Informational	Destroy, Disrupt, Delay	Security	JIPB/JOPES/Targeting Process	Individuals, Governments, Militaries
	Computer Network Defense	Physical, Informational	Protect Computer Networks	Security	JOPES/J-6 Vulnerability Analysis	Individuals, Businesses, Governments, Militaries
	Computer Network Exploitation	Informational	Gain Information From and About Computers and Computer Networks	Security	JIPB/Targeting Process	Individuals, Governments, Militaries
Psychological Operations	Psychological Operations	Cognitive	Influence	Relevance	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Military Deception	Military Deception	Cognitive	Mislead	Accuracy	JOPES/Joint Operation Planning	Militaries
Operations Security	Operations Security	Cognitive	Deny	Security	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Supporting Capabilities	Information Assurance	Informational	Protect Information and Informatin Systems	Security	JOPES/J-6 Vulnerability Analysis	Businesses, Governments, Militaries
	Physical Security	Physical	Secure Information and Information Infrastructure	Usability	JOPES/Defense Planning	Businesses, Governments, Militaries
	Physical Attack	Physical	Destroy, Disrupt	Usability	JOPES/Joint Operation Planning	Governments, Militaries
	Counterintelligence	Cognitive	Mislead	Accuracy	JIPB/Human Intelligence Collection	Governments, Militaries
	Combat Camera	Physical	Inform/Document	Usability, Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
Related Capabilities	Civil Military Operations	Cognitive	Influence	Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
	Public Affairs	Cognitive	Inform	Accuracy	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
	Public Diplomacy	Cognitive	Inform	Accuracy	Interagency Coordination	Governments

Figure 9—Source Joint Publication 3-13, Information Operations

AFIT is in a unique position to capitalize on its experience in both of these areas. Conversations with professors and fellow IDE classmates provided a great deal of insight as to what they believe would be a good blend of current existing courses to cover the

operational cyber warrior spectrum. Additionally, I borrowed the notional concept of information operations integration into joint operations (see Figure 9) to match our cyber operations course with what the Joint Operators consider important. Obviously the Computer Network Operations readily lends itself to the cyber realm, but there are other activities, such as, information assurance which also needs to be included. Additionally if other traditional IO roles use cyberspace to get their mission accomplished then they have become cyber warriors also.

Final Recommendations

Presented in Figure 8 are the core courses considered to be most pertinent to a future IDE cyber warfare student with an operational focus.

Course Number	Course Title	Course Credit Hours	Course Requirement
SENG 520	Systems Engineering Design	4	
SENG 535	Military Space Systems and Applications	1	TS/SCI
CSCE 525	Introduction to Information Warfare	4	
CSCE 544	Data Security	4	
CSCE 528	Cyber Defense Exercise 1	4	IMGT 658
CSCE 628	Cyber Defense Exercise 2	4	IMGT 658
EENG 574	Command, Control, Communications and Computer (C4) Warfare	4	NOFORN
IMGT 580	Enterprise Information Architecture	3	
IMGT 657	Data Communications for Managers	3	
IMGT 658	Local Area Networks	3	
IMGT 669	Business Process Improvement	3	
IMGT 680	Knowledge Management	3	
IMGT 687	Managerial Aspects of Information Warfare	3	
IMGT 688	Security and Ethics in the Information Age	3	
	Total Hours:	46	

Figure 10—Proposed Curriculum for IDE Cyber warrior Track

One can readily see that the proposed curriculum crosses several cultural domains. This considered essential and desirable to make a “well-rounded” cyber trooper. Obviously,

as with any type of curriculum development, the cyber warrior track can and should be further refined and tailored to meet the ever changing needs of the warfighter.

Some important observations noted during this selection process were:

1) The CSCE 525 course should probably be split into 2 separate classes. (e.g. Information Warfare 1 and Information Warfare 2). This was suggested because there was too much information to adequately cover in only one quarter.

2) There were some concerns with material overlap between the CSCE 525 class and the IMGT 687 class. This shouldn't be a concern, because IMGT 687 is primarily focused on the risk assessment, security practices, crisis response, and disaster recovery of information technology systems.

3) The IMGT 688 class needs to have more in-depth focus on the legal issues, and potential legal issues of cyber warfare. As noted earlier in this paper, what are the legal consequences if a weapon aimed at an adversary affects a neutral country?

As stated before, AFIT's unique capabilities and expertise have it primed to be a center of excellence for educating cyber warriors at the operational level of warfare. With due diligence and input from Air Force and Joint operators, AFIT will be extremely successful in providing what is needed to prepare the cyber warriors of the future.

Conclusion

The SECAF and CSAF mandated that the Air Force will do battle in cyberspace as per our 7 Dec 05 mission statement. This new medium requires that we understand who our enemies are, and what they can do with the cyber tools at their disposal. It also requires that we, as warriors, are on the same sheet of music in our collective knowledge and understanding of what cyberspace is, and what it can bring to the fight. Because this is the "bleeding" edge of combat operations, the Air Force needs to create an educational program for a new class of IDE warrior. This warrior must not only understand some of the technical aspects of cyberspace, but also understand the operational impact of cyber warfare to future conflicts. Additionally, cyber warriors must start concentrating on the information aspect of cyberspace. Failure to do so will result in faulty process development, communications breakdowns and misunderstandings, and underperforming technology solutions to move the information.

Because of these tall requirements, AFIT is uniquely situated to start educating IDE students in this type of operational thinking. There are classes currently being taught that could fulfill some of the requirements needed, but a paradigm shift is needed to ensure the IDE students are receiving the right material at the right level. Enclosed in this report are the collective thoughts of IDE students and some professors as to the type of curriculum that needs to be included in the cyber warfare track. Ubi concordia, ibi victoria. (Where there's unity, there is the victory).

Bibliography

1. Michael Wynn and T. Michael Mosely, Letter to the Airmen of United States Air Force, 7 Dec 2005

2. Maj Scott D. Tobin, *Establishing a Cyber Warrior Force*, AFIT Thesis, Sep 2004

3. William Gibson, *Neuromancer*, Penguin Group, 1984.

4. http://www.whatis.com

5. Eric A. Fisher, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, Congressional Research Service RL 32777, The Library of Congress, 22 Feb 2005.

6. Department of Defense, Quadrennial Defense Review Report, 6 Feb 2006

7. John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, Congressional Research Service RL 33123, The Library of Congress, 20 Oct 2005.

8. "UK Hacker Should be Extradited," BBC News, (10 May 2006); available from http://news.bbc.co.uk/2/hi/technology/4757375; accessed 15 May 2006.

9. US Army Training and Doctrine Command, DCSINT Handbook No. 1.02, *Cyber Operations and Cyber Terrorism*, 15 Aug 2005.

10. John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, RL 33123, Congressional Research Service, The Library of Congress, 20 Oct 2005.

11. Clay Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, RL32114, Congressional Research Service, The Library of Congress, 17 Oct 2003.

12. Gabriel Weimann, *Cyberterrorism How Real Is the Threat?*, United States Institute of Peace, Special Report 119, December 2004.

13. John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, RL 33123, Congressional Research Service, The Library of Congress, 20 Oct 2005

14. Gabriel Weimann, *Cyberterrorism How Real Is the Threat?*, United States Institute of Peace, Special Report 119, December 2004.

15. Thomas J. Barrett, *National Cyberguard; Defending America's Cyberspace against the Strategic Threat*, National Center at Norwich University-Applied Research Institute, 2005

16. Mark Rasch, "Why the Dogs of Cyberwar stay leashed", SecurityFocus Online, 24 March 2003, accessed from www.theregister.co.uk.

17. Col Qiao Liang and Col Wang Xiangsui, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, China, February 1999.

18. US Army Training and Doctrine Command, DCSINT Handbook No. 1.02, *Cyber Operations and Cyber Terrorism*, 15 Aug 2005.

19. Dr. Robert Mills and Dr Richard Raines, "Producing IA, IO, and Cyber warriors" briefing to BG Miller, 20 April 2006

20. *The National Strategy to Secure Cyberspace*, February 2003.

21. Maj Scott D. Tobin, *Establishing a Cyber Warrior Force*, AFIT Thesis, Sep 2004

22. Lionel Galway, Richard Buddin, Michael Thirtle, Peter Ellis, and Judith Mele, *Understrength Air Force Officer Career Fields*, Rand Corporation, 2005.

23. Leigh Armistead, *Information Operations*, Brassey's Inc., Washington D.C., 2004.

24. Dr Jeff Grossman, and Richard Akita, "Global Threats Demand Credible Response in Less Time", Signal Magazine, March 2006.

25. John Gilligan, Chief Information Officer United States Air Force Statement Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities House Armed Services Committee United States House of Representatives, 3 April 2003.

26. Allan Holmes, "Federal IT Flunks Out", CIO Magazine, 15 May 2006.

27. Joint Publication 3-13, *Information Operations*, 13 February 2006.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
13-06-2006	Graduate Research Project	Mar 2006 – Jun 2006

4. TITLE AND SUBTITLE

COURSE CURRICULUM DEVELOPMENT FOR THE FUTURE CYBERWARRIOR

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Chacon, Mark A., Major, USAF

5d. PROJECT NUMBER

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, Building 640
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/IC4/ENG/06-02

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

Dr Robert Mills
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

On 7 December 2005, the Secretary of the Air Force (SECAF) changed the Air Force's mission statement to include operations in Cyberspace. The implication of this change is that the Air Force will need to educate, train, and equip its forces to operate on this new battlefront. To this effect, IDE cyber warfare officers will need to understand the processes, technology, and legal ramifications of operating in this new realm. AFIT is in a unique position to modify and develop new curriculum to support the SECAF's strategic vision. Because of its warfighting focus, AFIT can provide courses that optimally prepare future cyber warriors. This GRP will focus on the demographics and types of courses needed to make a well rounded "cyber trooper".

15. SUBJECT TERMS

Cyber, Warrior, Curriculum Development

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr Robert F. Mills, ENG
U	U	U	UU		19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4527 (richard.raines@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18