

A Training Regimen for Incoming USAF Employees

John Bommer
Lt Col, Commander, 26 Network Operations Squadron
Charneice McKenzie
2nd Lt, 26 Network Operations Squadron
Gary Rogers
Trainer, 26 Network Operations Squadron
Maxwell-Gunter Air Force Base
490 E. Moore Street,
MAFB-Gunter Annex, AL 36114
rogersgator@maxwell.af.mil

Table of Contents

Training and Education	108
The Environment and Role of the United States Air Force in Training for a Cyberspace Role	113
The Specific Role and Training Methods of the 26 Network Operations Squadron	122
Appendices	
Appendix A: IQT Example: Classified Handling	125
Appendix B: MQT Example 1 – Security	126
MQT Example 2 – Security	129

The Importance of Training

Effective training benefits both the employee and the organization. On the employee side, most, if not all, employees want to be valuable and remain competitive in the labor market. A major method of achieving this is effective employee training and development. Not only one-time training but recurring training that will result in a continued well-trained and effective workforce while at the same time meeting legal and regulatory requirements. On the employer side, especially in the current tight labor market, employees want to develop career-enhancing skills, which will, in turn, lead to employee motivation and retention, both “pluses” for any organization public or private. There is no doubt that a well trained and developed staff will be a valuable asset to the company and thereby increasing the chances of his efficiency in discharging his or her duties. Specifically, why? The right employee training, development and education can result in significant payoffs for the employer in increased tangibles such as productivity, and intangibles such as loyalty, knowledge, and contribution to the organization.¹

Training and Education

First, let us briefly examine the differences between training and education. Formal education is typically envisioned as the process of studying a series of subjects in schools, whether they be primary schools or major universities. According to Census 20002, more than one-fourth of the U.S. population aged 3 and older attended school in the spring of 2000. The 76.6 million students included 5.0 million enrolled in nursery school, 4.2 million in kindergarten, 33.7 million in elementary school, 16.4 million in high school, 14.4 million in college (undergraduate), and 3.1 million in graduate school. Most if this is formal education. Of course, this leads us to the conclusion that age is not necessarily a relevant factor here, namely that the age of a student undergoing formal education can range from age 4 through adulthood. The students range from the very youngest through college to those in adult education. For example, Nola Ochs is a **continuing education** student at the Fort Hays State College in Kansas. Nola has her own apartment on campus where she attends classes, and when she's able to get home for the weekend, she drives 100 miles home her family farm. She is scheduled to graduate with a bachelors degree this spring. Nola turned 95 in November.³

The objective of classes, of course, is typically to gain knowledge about facts, events, principles, concepts, etc. How is this skill demonstrated? Many times the learner is required to demonstrate the memorization of facts and the association between concepts. In other cases, they must apply rules to solve problems. Also, there is the issue of assessments, commonly known as testing.

1 “Importance Of Training And Development In A Firm”, by [Ndunuju Adiele](#) , <http://ezinearticles.com/?Importance-Of-Training-And-Development-In-A-Firm&id=1885451>.

2 School Enrollment 2000, <http://www.census.gov/prod/2003pubs/c2kbr-26.pdf>

3 “Oldest College Graduate In The US”, by Pam Sissons, March 21, 2007, http://www.suite101.com/blog/adirondack/oldest_college_graduate_in_the_us

Testing addresses the skills of memorization and understanding, plus perhaps analytic and problem solving skills.⁴

Fundamentally, training is usually centered around the concept of obtaining a skill. Training is typically conducted in trade schools, technical institutes, seminars, and business training classes. Apprenticeships also are evident here in order to provide on the job training, a crucial aspect of the training process. The age range in this mode ranges from the very young to the very old, similarly to formal education. Apprenticeship programs vary throughout the U.S. For example, the U.S. Department of Labor offers a Registered Apprenticeship program to assist prospective apprentices and employers in this arena and offers access to 1,000 career areas, including the following top occupations:⁵

- Able seaman
- Carpenter
- Chef
- Child care development specialist
- Construction craft laborer
- Dental assistant
- Electrician
- Elevator constructor
- Fire medic
- Law enforcement agent
- Over-the-road truck driver
- Pipefitter

In short, education concerns remembering facts and understanding concepts. It is usually taught in school. Training concerns gaining skills and taught either in trade schools or business training sessions.⁶

This being said, these do have a common trait, namely that training and education are both different facets of learning. At first, it may be difficult to tell the difference between them, especially in today's school system, but there are major differences in training and education. Their purpose, history, and methodology are all vastly different.⁷

4 "Difference Between Education and Training", by Ron Kurtus, October 12, 1999, <http://www.school-for-champions.com/training/difference.htm>

5 U.S. Department of Labor, U.S. Employment and Training Administration, <http://www.doleta.gov/oa/apprentices.cfm>

6 "Difference Between Education and Training", by Ron Kurtus, October 12, 1999, <http://www.school-for-champions.com/training/difference.htm>

7 "Difference Between Education and Training", <http://www.differencebetween.net/miscellaneous/difference-between-education-and-training/#ixzz0lfPsvvwS>

Purpose

Training – is undertaken in the hopes of gaining a specific skill. Generally this skill will make you more employable. These skills can be manual such as the ones listed above by the U.S. Department of Labor.

Education – is undertaken in the hopes of furthering your individual knowledge and developing your intellect. While a highly educated person is often more employable, education is not about getting a job.

History

Training – was originally practiced through guilds. Youngsters would be apprenticed to a master baker, builder or blacksmith and then work under him, sometimes for decades, in order to learn his trade. This was considered the appropriate and most effective method of learning for the lower and middle classes, if one was lucky. In most cases, young men were not selected into these programs and so died at an early age.

Conversely, education has its origins in the medieval university system. Young men from wealthy families would complete a course in theology or philosophy before studying his chosen profession (women didn't generally enter this picture until much later). In fact, the educational progress of women did not occur until many centuries later. For example, "the education of Noble women in the Middle Ages concentrated on the practical as opposed to academic. Young noble women as young as seven girls would be sent away from their home to live with another noble family. There she would be taught a range of subjects and skills. Manners and etiquette were of prime importance, including how to curtsy and how to mix with the greatest nobles in the land. Time would be spent learning how to dance and ride. Archery were also taught to young noble women. These young girls were expected to act as servants to the older ladies of the castle. The duties of the young noble women would be to look after clothes and the assist ladies with their dressing and coiffure. Some housewifely duties such as preserving fruits and household management would be taught, to prepare them for their duties as a married woman. High ranking young women would take on the role of ladies-in-waiting and were taught French. Young noble women would also be taught the principles of the Medieval Code of Chivalry and Courtly Love and would join the spectators at jousting tournaments."⁸ "Their role greatly expanded during the Renaissance. During that age, women had a significant impact on the economy, social structures, and the culture of the Renaissance, despite the constraints on their exercise of power, lack of opportunities, enforced dependence, and exclusion from politics, government, science, law, banking, and more."⁹ Even though women's roles in these arenas expanded during this period, it is still true that the power of men was almost absolute and remained that way. Arguably, this trend is still evident today, but major strides are being made. For example,

8 "Noble women in Middle Ages", <http://www.middle-ages.org.uk/noble-women-in-the-middle-ages.htm>

9 Brown, M., McBride, Kari. 1995. *Women's Roles in the Renaissance*. Santa Barbara: Greenwood Press.

Nearly six out of ten adults holding advanced degrees between the ages of 25 and 29 are women.¹⁰

In today's myriad educational system, the line between education and training can be very fine indeed. Especially at the collegiate level, many areas of mental training are being passed off as education. Programming, for instance, requires a difficult and specialized skill set and needs years of training. Even fields previously thought of as "training" such as heating and air conditioning, now, due to the pervasiveness of complex technology inherent in the devices utilized in this field, require a great deal of what is known as formal education.

The USAF: Education and Training: Some Differences¹¹

A CONTINUING debate exists as to the distinction between *education* and *training*. In everyday conversation, people frequently use the terms interchangeably. Indeed, there are some, I suspect, who believe that the best approach to the problem of differentiating between education and training is to ignore the distinction. I do not share this view.

For many years the U.S. Air Force drew a clear distinction between education and training. Education was organized under Air University; training, under Air Training Command. Then, in 1978, the Air Force consolidated education and training under the same major air command structure. In 1983, USAF leaders decided again to draw a clear distinction between education and training, reintroducing a major air command structure to administer each. The decision was a good one, for although there are similarities between education and training, there are some basic differences—differences which Air Force curriculum developers and instructors should keep in mind.

Following the traditional three-part distinction among the domains of learning (psychomotor or doing, cognitive or thinking, affective or feeling), training emphasizes the psychomotor domain of learning. Training that is done in the cognitive domain is generally at the knowledge level and lower part of the comprehension level. Education, on the other hand, teaches a minimum of psychomotor skills. It concentrates instead on the cognitive domain, especially the higher cognitive levels, i.e., high comprehension and above. Affective learning, by the way, may be a product of both education and training.

Criterion objectives are most appropriate for training. That is, under a given set of conditions, a student will exhibit a specific behavior to a certain predetermined level or standard (e.g., "without the use of references, list the steps of the USAF Instructional System Development Model according to AFM 50-2, in order and without error"). Cognitive objectives written at the appropriate level of learning (knowledge, comprehension, application, analysis, synthesis, or evaluation) are more useful for education. When behavioral or criterion objectives are used in education, they are generally broader than when used in training and relate to the learners' ability to

10 "More women than men get advanced degrees", by Stephanie Chen, April 20, 2010,

<http://www.cnn.com/2010/LIVING/04/20/census.women.advanced.degrees/index.html?hpt=Sbin>.

11 Education and Training: Some Differences, John Kline, verbatim, <http://www.airpower.maxwell.af.mil/airchronicles/aureview/1985/jan-feb/kline.html>

generalize, see relationships, and function effectively in new situations—situations which cannot be completely visualized or defined.

Training is essentially a closed system. The trained individual is easily recognized as knowing the "right answers," doing things the "approved way," or arriving at the "school solution." Under these conditions, the products of each trainee in every situation can be expected to look the same. Education, in contrast, is an open system. Learning is continuous with no cap or ceiling on how well the graduate may be prepared to handle new responsibilities. Right answers and ways of doing things often do not exist in education—only better or worse ones.

Objectives, job requirements, and skill levels are constraints with training. Yet time required for training can vary because of the aptitude, experience, and previous skill level of the student. With education, however, time is often a constant (four years, ninety semester hours, ten months, forty hours in class) and therefore is specified. This is not to say that one's education is ever complete. It is not. However, to fit time constraints, objectives in education must be selected from a much wider range of possible objectives than can ever be included in the time available, due to the nearly infinite combination of position responsibilities of the graduates. Objectives, job requirements, and skill levels are not constraints with education, since persons are encouraged to develop to their potential.

With training, a task analysis can be done so that the curriculum will include a complete listing of skills and knowledge required for the graduate to demonstrate competence. With education, curriculum planners and instructors must select a sample to teach from a universe of ideas. Furthermore, they must often rely on opinion from acknowledged, credible experts to determine what needs to be taught. Creative, visionary experts are needed to predict future needs rather than merely reflect current ones. This absence of exactness often results in a lack of consensus on what should be taught. Analyze courses taken by majors in a given field or discipline at different universities, and you will find differences. For that matter, you will find differences among curricula of the various senior and intermediate service schools. Differences in curricula and emphasis on individual study are good in education but usually not in training.

These differences between education and training do not suggest that one facet of learning is more important than the other, only that they are different. Obviously, genuine accomplishment (competence, proficiency, good judgment, effectiveness) incorporates both. A person cannot, for example, effectively give a speech, fly an airplane, edit a scholarly journal, or command an Air Force organization without a wide range of knowledge and skills. Still, these differences have strong implications for those who provide education or training. Failure to acknowledge them will hinder learning and, ultimately, performance. Recognizing their relevance in curriculum planning and teaching will improve both education and training in the United States Air Force.

The Environment and Role of the United States Air Force in Training for a Cyberspace Role

Foreword

Cyberspace is a critical global domain, in which the USAF will conduct integrated operations in support of Joint Force Commanders' needs. The United States is not alone in recognizing the asymmetrical advantages of this domain. Potential adversaries worldwide are rapidly improving or pursuing their own cyber capabilities. Attempts to disrupt or penetrate our networks are relentless. To address these issues, the USAF has developed The United States Air Force Blueprint for Cyberspace, dated November 2, 2009. This document provides a framework to meet these challenges by evolving the Air Force culture and improving its capabilities. Air Force Space Command as the lead USAF Major Command (MAJCOM) for cyberspace is charged with executing this blueprint as a unified effort--working closely within the Air Force, and with sister services, combatant commands, Joint Staff and other partners in order to fully provide the necessary capabilities for the future.

Tenets of the USAF Blueprint for Cyberspace

Current Situation

Cyberspace touches practically everything and everyone every day. The security and prosperity of our nation is dependent on freedom of access to and freedom of action in cyberspace. While there are many benefits that come with this access, there are numerous inherent vulnerabilities. Threats via cyberspace pose one of the most serious national security challenges of the 21st Century. The threat is asymmetrical with a minimal cost of entry; events of the last several years show that one person, with one computer, can affect an entire nation. Growing arrays of adversaries are targeting the US military and our critical national infrastructure, commerce and citizens. The combined and coordinated efforts of government, industry and academia will be required to effectively counter many of these attacks and assure mission success in the future.

Presidential Guidance

In May 2009, the White House released the "Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure". While the White House review sought primarily

"to assess US policies and structures for cyber security," it examined "the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."

12

12 "Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure", May 2009, The White House, Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure.

The review acknowledged “America’s failure to protect cyberspace [as] one of the most urgent national security problems facing the new administration” and that “protecting cyberspace will require changes in policies, technologies, education and perhaps laws.”

On the technology front, the review concluded “existing solutions can only do so much given the underlying design of the Internet architecture,” and cited an advisory group for the Defense Advanced Research Projects Agency (DARPA) as saying, “the defense of current Internet Protocol-based networks as a losing proposition and called for an independent examination of alternate architectures.” The President called for the federal government to work with industry on the development of “next-generation secure computers and networking for national security applications.”

Specifically, the globally-interconnected digital information and communications infrastructure known as “cyberspace” underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security.¹³ It is certainly true that information technology has transformed the global economy and connected people and markets in ways never imagined. In order to realize the full benefits of this digital revolution ¹⁴, users must have confidence that sensitive information is secure, commerce is not compromised, and the infrastructure is not infiltrated. Since this digital revolution is so profound, this is indeed a major challenge.¹⁵

Nations also need confidence that the networks that sustain their national security and economic prosperity are safe and durable. It is clear that achieving a trusted communications and information infrastructure will guarantee that the United States achieves the full potential of the information technology revolution. The December 2008 report by the Commission on Cybersecurity for the 44th Presidency states the challenge plainly: “America’s failure to protect cyberspace is one of the most urgent national security problems facing the new administration.”¹⁶

Protecting cyberspace requires strong vision and leadership and will require changes in policies, technologies, education, and regulatory, criminal and civil law. Only via demonstrating commitment to cybersecurity-related issues at the highest levels of government, industry, and civil society will allow the United States to continue to lead innovation and adoption of cutting-edge technology, while at the same time improving national security and its global standing and economy.

13 Office of the Presidency, U.S. Government, “*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*”, May 9, 2009.

14 The New Geography: How the Digital Revolution Is Reshaping the American Landscape, Joel Kotkin, 1991, New York: Random House.

15 <http://library.thinkquest.org/25744/index.htm>.

16 CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, December 2008, at 11.

Case for Action

Threats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies. A growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government. For example, on March 25, 2010, one of the world's most notorious computer hackers, Albert Gonzalez, was sentenced to 20 years in prison after he pleaded guilty to helping run a global ring that stole tens of millions of payment card numbers. It was the harshest sentence ever handed down for a computer crime in an American court. Gonzalez and conspirators scattered across the globe caused some \$200 million in damages to those businesses.¹⁷

These actors have the ability to compromise, steal, change, or completely destroy information.¹⁸ The continued exploitation of information networks and the compromise of sensitive data, especially by nations, leave the United States vulnerable to the loss of economic competitiveness and the loss of the military's technological advantages. As the Director of National Intelligence (DNI) recently testified before Congress, "the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures."

The Intelligence Community assesses that a number of nations already have the technical capability to conduct such attacks.¹⁹ Several nations are known or suspected to have this capability to include China, North and South Korea. Attacks originated in China lately have been pervasive in the news. Researchers from the University of Toronto have uncovered a network of hackers, centered in China, which has used popular online services to obtain top secret information from the Indian government, many centered around Tibetan dissident groups and the Dalai Lama. The researchers stated that they were able to observe the cyber attacks and traced them to servers located in China, and specifically to individuals located in the city of Chengdu--the home of the communist country's military intelligence collection/technical reconnaissance bureaus. These attacks uncovered "complex ecosystem of cyber espionage that systematically compromised government, business, academic and other computer networks in India, the Offices of the Dalai Lama, the United Nations, and several other countries."²⁰ And India is not alone. Australia has also felt this effect. Firms in that country have recently been hit by hackers originating in China,

17 Albert Gonzalez, '\$200 million damage' hacker, sentenced, Reuters, <http://www.independent.co.uk/life-style/gadgets-and-tech/news/albert-gonzalez-200-million-damage-hacker-sentenced-1928313.html>

18 Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record*, March 10, 2009, at 39.

19 Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record*, March 10, 2009, at 39.

20 *Shadows in the Cloud, Investigating Cyber Espionage*, April 6, 2010, Shadowserver Foundation, University of Toronto.

one time even dramatically slowing that nations' second largest broadband network.²¹ And the recent censorship debate between Google and the Chinese government has resulted in series of hacker attacks on both Google and Chinese dissent groups living abroad.²² China is not the only culprit. Hackers originating in Russia also are active. For example, denial-of-service (DOS) attacks against Web sites in Estonia have been increasing lately. The attacks crippled Web sites for Estonia's prime minister, banks, and less-trafficked sites run by small schools, said Hillar Aareleid, chief security officer for Estonia's Computer Emergency Response Team (CERT). Hackers sponsored by the Russian government are suspected. Press reports also speculated that tension between the two countries may have resulted in a coordinated campaign by Russia against Estonia. Last month, Estonia irked Russia by moving a Soviet-era World War II memorial of a bronze soldier, sparking protests.²³ North Korea has also been active in this regard. A series of attacks on computer networks in South Korea and the US was apparently the work of North Korean hackers. The attacks, which targeted the White House, the Pentagon, and the Washington Post, among other high-level institutions, are raising concerns that the long-simmering conflict with North Korea is expanding into a dangerous new theater.

The Associated Press obtained a list of the targets in the attack. Included on the list are the National Security Agency, the Department of Homeland Security, the State Department, and the Nasdaq stock exchange. In South Korea, the sites of the presidential office, the defense ministry, and the National Assembly were targeted. Many analysts see the attacks as a test of the US government's ability to deal with a coordinated cyber-attack.²⁴²⁵

The growing sophistication and breadth of criminal activity, along with the harm already caused by cyber incidents, highlight the potential for malicious activity in cyberspace to affect U.S. competitiveness, degrade privacy and civil liberties protections, undermine national security, or cause a general erosion of trust, or even cripple society. For example:

- Failure of critical infrastructures. CIA reports malicious activities against information technology systems have caused the disruption of electric power capabilities in multiple regions overseas, including a case that resulted in a multi-city power outage.²⁶
- Exploiting global financial services. In November 2008, the compromised payment processors of an international bank permitted fraudulent transactions at more than 130 automated

21 "Chinese cyberattack targets Australia", by Rohan Sullivan, April 15, 2010, <http://www.physorg.com/news190524906.html>

22 "Chinese Human Rights Sites Hit", by Owen Fletcher, http://www.peworld.com/businesscenter/article/187597/chinese_human_rights_sites_hit_by_ddos_attack.html

23 "Estonia recovers from massive denial-of-service attack", by Jeremy Kirk, <http://www.infoworld.com/d/security-central/estonia-recovers-massive-denial-service-attack-188>

24 "North Korean hackers blamed for sweeping cyber attack on US networks", by Matthew Shaer, July 8, 2009, <http://www.csmonitor.com/Innovation/Horizons/2009/0708/north-korean-hackers-blamed-for-sweeping-cyber-attack-on-us-networks>

25 "South Korea again hit by cyber-attacks, as search for hackers intensifies", by Matthew Shaer, July 9, 2009, <http://www.csmonitor.com/Innovation/Horizons/2009/0709/south-korea-again-hit-by-cyber-attacks-as-search-for-hackers-intensifies>

26 www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5, CIA presentation, SANS SCADA Security Summit, January 16, 2008.

teller machines in 49 cities within a 30-minute period, according to press reports.¹⁴ In another case reported by the media, a U.S. retailer in 2007 experienced data breaches and loss of personally identifiable information that compromised 45 million credit and debit cards.²⁷

• Systemic loss of U.S. economic value. Industry estimates of losses from intellectual property to data theft in 2008 range as high as \$1 trillion.²⁸ • losses due to criminal gangs. criminal gangs are increasingly committed to cyber crime, even recruiting promising young people as young as 14.²⁹ Why? The possibilities of potential earnings over the internet are roughly unlimited and the reasonable securities which the Internet sources provide are not sufficient to catch these criminals. In fact, it is reported that cyber crime has been one of the main income earnings for many criminal gangs.³⁰

DoD Guidance on Cyberspace

The Department of Defense (DOD) defines cyberspace as “a global domain within the information environment...” Cyber operations are defined as “the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace; such operations include computer network operations and activities to operate and defend the GIG.”

The President’s Unified Command Plan assigns United States Strategic Command (USSTRATCOM) the mission to conduct cyberspace operations. To fulfill the President’s vision, the Secretary of Defense (SECDEF) tasked USSTRATCOM to establish the sub-unified US Cyber Command (USCYBERCOM). Subsequently, the USSTRATCOM Commander directed the development of an overarching vision and unified framework to synchronize and integrate global cyberspace operations. This direction compliments the Joint Chiefs’ of Staff GIG 2.0 concept calling for the integration of service specific cyber infrastructures into a common enterprise; organized, trained and equipped to support the Joint Force Commanders. Thus, the intent for USCYBERCOM is to direct operations and defense of specified DOD information networks and conduct full spectrum military cyberspace operations in order to enable actions in all domains. In response, each of the military services is aligning its organizations and capabilities to support the SECDEF’s direction.

USAF Intent

The significance of USAF operations in cyberspace is readily apparent. Not only is cyberspace vital to today’s fight, it is key to the continued US military advantage over our enemies, now and in the future. Consequently, the USAF is steadfastly intent on providing a full range of cyber

27 www.infoworld.com/d/security-central/retailer-tjx/reports-massive-data-breach-952, January 17, 2007.

28 www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html. See also <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>, McAfee, “Unsecured Economies: Protecting Vital Information”, January 2009. Projection based on survey by Purdue’s Center for Education and Research in Information Assurance and Security.

29 Criminals target tech students, December 8, 2006, <http://news.bbc.co.uk/2/hi/6220416.stm>

30 A Short Summary of Cyber Crime, August 28, 2008, by AnindyaSundar Mandal, <http://www.ecademy.com/node.php?id=110978>

capabilities to Joint Force Commanders, whenever and wherever needed. Today, USAF cyber capabilities range from the virtual to the very real, including critical combat communications provided to the warfighter within hours upon the arrival of the USAF. The USAF will move forward aggressively to:

- Consolidate and protect the USAF portion of the DOD network
- Build capacity by increasing the skill of our people, generating innovative operational capabilities, leveraging new partners and integrating those capabilities with those in the air and space.³
- Expedite requirements and acquisition processes to deliver proactive and responsive cyber capabilities
- Develop doctrine, policies, security and guidance to effectively employ and innovate in cyberspace
- Prioritize and advocate for needed resources for cyberspace
- Significantly increase intelligence and analytical capabilities
- Shift paradigms from network-focus to mission-focus
- Develop cyber expertise to meet mission needs
- Improve commanders' decision making abilities by increasing situational awareness
- Affect changes in behavior, practices and culture by improving training, standards, communication and accountability
- Modernize and sustain the technology and equipment used for combat communications
- Eliminate seams in command and control (C2), security and doctrine to improve cross-domain effectiveness
- Combine and converge traditional operations with cyberspace operations to deter attacks and affect outcomes
- Partner with the DOD and other services to integrate, synchronize and consolidate the network infrastructures used by the joint forces

Commander's Guidance

The USAF will contribute to the joint fight by organizing, training and equipping expeditionary-capable cyber forces which will be presented to USSTRATCOM, USCYBERCOM, and other Combatant Commanders (COCOMS) as needed to conduct full spectrum operations. Consistent with joint terminology, operating concepts and views on the joint operating environment, the USAF views cyberspace as a contested operational domain that pervades and enables capabilities and effects in all other operational domains.

Cyberspace is persistent, real-time and inherently global. USAF operations in the air, space and cyberspace domains are interdependent and focused on the needs of the Joint Force Commanders. The USAF will protect cyber capabilities and integrate them with other domains to enable joint warfighting effects greater than the sum of their parts. The protection of the USAF portion of the DOD network architecture will focus on mission assurance. Until now, US adversaries have faced little to no risk or consequence in attacking or exploiting our systems, and the response has been to build stronger "walls." The time has come to think of cyberspace in a new light; not only must we defend against any attack, we must be able to "fight through" any attack, accomplish our missions and retain the ability to respond—thus giving us mission assurance in the face of future attacks or other disruptions.

Under the direction of the Commander, US-CYBERCOM, the Air Force will prepare and conduct a dynamic defense with a range of responsive capabilities enabling flexible strategic and operational response options for the combatant commanders. The USAF will assess network vulnerabilities and threats by mapping mission dependence on cyberspace, mission essential functions and supporting infrastructure. Additionally, the USAF will leverage its space and air assets to create redundancies for mission assurance and critical infrastructure needs while ensuring cross-domain tactics, techniques and procedures (TTPs) are effective and consistent. Training and standardization and evaluation programs will reflect the operational mission focus and the combat mission readiness status of USAF cyber forces.⁴

The USAF will continue to improve security of existing cyber infrastructure while pursuing a next generation network architecture that is integrated, mobile, visual, virtual, secure, responsive and intuitive. Currently, the joint community and COCOMS are supported by a multitude of decentralized network infrastructures operated by the services, contractors and industry, most running different configurations of the same programs, which is costly, complex and difficult to defend. It is both necessary and inevitable to integrate and synchronize these networks while transitioning to a single seamless network. The USAF will seek a single, integrated network encompassing air, terrestrial, and space layers that is managed and commanded/controlled as a single entity and that is fully compatible with a seamless DOD network. Cyber operators must be able to employ this common architecture and associated technologies for the full range of cyberspace operations, and to do so seamlessly with those of our mission partners. This next-generation architecture will enable exponential increases in capabilities for every mission and increase synchronization and real-time global situational awareness. It is estimated that in the next decade an Airman will carry in his hand 10 times the computing power of his current desktop, laptop and phone combined. It is the goal of the USAF to ensure each Airman has access to leading-edge technology and connectivity through an assured next-generation network.

The USAF Concept of Operations

In October 2008, the Secretary of the Air Force designated Air Force Space Command (AFSPC) as the USAF lead MAJCOM for organizing, training and equipping cyber capabilities. This alignment allows the USAF to focus its efforts and capitalize on inherent synergies found in space and cyberspace architectures and processes. Additionally, the USAF established a new cyberspace operational Component Numbered Air Force (C-NAF) under AFSPC. In August 2009, the USAF activated the 24 AF as its operational cyberspace entity with the responsibilities to integrate, employ and consolidate cyber capabilities in support of Joint Force Commanders and USAF component commander needs.²⁴ AF is the USAF's cyber warfighting organization and has the requisite capabilities and authority to establish, operate, maintain and defend USAF networks, conduct other operations as required and present cyber forces and capabilities to USCYBERCOM and the other combatant commanders as required. The 24 AF Commander serves as the USAF component commander to USCYBERCOM and provides the operational focus, flexible command and control (C2) capability and single streamlined force to support Joint Force Commanders. To accomplish cyberspace missions and tasks, 24 AF is assigned three wings and is directly supported by the Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA).²⁴ AF Commander is also the Air Force Network Operations (AFNETOPS) Commander and, under the direction of the USCYBERCOM Commander, will execute C2 over the AF portion of the GIG. As a focal point for all AFNETOPS, 24 AF has established the 624 Operations Center to ensure that global network components essential for mission success are

defended, survivable and available to support air, space and cyberspace operations, and that cyberspace operations are integrated and synchronized with USCYBERCOM. The USAF will seek an expanded concept of operations that integrates air, space and cyberspace capabilities, streamlines command and control, advances doctrine and creates a security framework to facilitate integration and to allow cross-ideation for air, space and cyberspace.

New Style of Partnerships

Because of the shared risk and to reduce vulnerabilities, the USAF must establish new relationships and actively strengthen and expand its partnerships with interagency, joint, industry, academia and international entities. Cyberspace transcends military domains and national boundaries and has changed the way we interact globally. The USAF operates a small percentage of the global cyberspace infrastructure. Industry currently provides over 90% of the cyberspace infrastructure, which potentially correlates to DOD mission success. This necessitates that the USAF must continue to foster existing relationships to enable and support the execution of the mission while fulfilling national objectives. The USAF must create new patterns of interaction with the cyber research and innovation communities and anticipate and articulate new needs for the science and technology community. Rapid technology advancements inherent in this domain require the USAF to continually strive to pioneer the future by developing new partnerships with academia and industry. The USAF needs to rapidly exploit technical advances by establishing a continuous process for working with the science, industry and academic communities that form the leading-edge information technology sector to shape our activities in the cyberspace domain.

Capability Integration

The USAF will develop unique cyber capabilities that originate in its distinct missions and take full advantage of the integration of air, space and cyber capabilities. Each service brings its own cyber strengths and capabilities to the joint team and the nation. Since air, space and cyberspace are inextricably linked both operationally and technically, the potential exists to integrate capabilities across these domains to exponentially increase each other's power. This integration promises to give joint force commanders unrivaled global access, persistence, awareness and connectivity capabilities and to rapidly restore critical infrastructure via a cross-domain network-of-networks approach. The USAF will seek to develop cyber capabilities that complement those of other services and will explore the combination of cyber with other non-kinetic capabilities to achieve synergies. The speed and nature of operations in cyberspace domain dictates a fusion of mission competencies and skills. The traditional cyber tasks must be integrated to present a full spectrum of seamless and synchronized capabilities and operations. Airmen will stop thinking of themselves as operators, communicators, intelligence experts, etc. but rather as an integrated team of multi-disciplined well-trained cyber professionals with the technical and tactical skills needed to execute any and all missions. The USAF will revolutionize its operations by establishing an integrated cyber operations center that is fully integrated with those of our joint partners to serve as the intersection for a full range of cyber capabilities. Expeditionary cyber forces comprised of team members with the appropriate training and experience will provide leading edge, tailored capabilities to meet USAF component and Joint Force Commanders' needs worldwide, from Irregular Warfare to high-end conflict.

Like offense and defense in the other operational domains, operations and intelligence in

cyberspace must not be separated. The USAF will optimize the fusion of intelligence and operations by significantly expanding and exploiting the full range of our intelligence resources and analytical capabilities. It is the USAF's goal to move from situational awareness to situational comprehension and ultimately situational projection with data that is easily shared across organizational boundaries. Since there are many common operating pictures (COPs) being assembled across the services and agencies, it is desirable to improve and consolidate COPs while making relevant USAF tools and data available to the joint COPs. The USAF will work to integrate space and cyberspace indicators and warnings to develop an advanced early warning architecture across the AF-GIG. Seamless operations and the strength of USAF partnerships will act as force multipliers to build capacity.

Operational Responsiveness

The rapidly changing cyberspace environment demands that we create a new acquisition strategy that is predictive, adaptive and timely and keeps us on the cutting edge of new technology. COCOM needs will emerge quickly and our goal is to deliver operational capabilities at the speed of need; therefore, the USAF will improve the process of indentifying cyber requirements and delivering responsive cyber capabilities. The re-engineering of requirements and acquisition to better support COCOM needs necessitates a tiered approach to meet operational needs in this dynamic environment. Our cyber adversaries attack 24 hours a day, seven days a week, 365 days a year and act and react in real time. This reality requires real-time modifications to existing capabilities and also a rapid hours-to-weeks acquisition process to meet these constantly evolving threats. The USAF will develop requirement thresholds to determine whether the need is real-time, rapid or foundational. An agile and adaptive requirements process will ensure that the USAF is optimizing limited resources while responding to future operational demands.

Cyberspace Culture The USAF will strive to change its cultural mindset in the day-to-day execution of cyber operations. The importance of cultivating a new mindset cannot be overstated. It demands a fundamental shift in leadership that encourages creative, yet critical thinking and rewards innovative activities and solutions. Cyberspace does not function independently of other capabilities provided by the USAF or other DOD agencies. For example, the question of capability integration is broader than just the USAF and requires an understanding of how USAF cyber capabilities may leverage or be leveraged by the capabilities of the other military services and mission partners. In addition, the integration and acculturation of cyberspace must permeate doctrine development, accession and advanced training, professional military education, exercises, war games, recruitment and day-to-day operations. A cultural change is also critical in the USAF operation and defense of the AF-GIG. Every USAF airman, government civilian, and contract partner must become a cyber defender. The United States is vulnerable to cyber attacks by relentless adversaries attempting to infiltrate our networks- at work and at home- millions of times a day, 24/7 planting malicious code, worms, botnets and hooks in common websites, software and hardware, such as thumb-drives, printers, etc. Once implanted, this code begins to distort, destroy and manipulate information, or "phone" it home. Certain code allows US adversaries to obtain higher levels of credentials to access highly sensitive information. Adversaries attack computers at work and at home knowing Airmen communicate with the AF network via email or transfer information from one system to another.

Airmen have a critical role in defending the USAF networks. They can significantly decrease the adversary's access to the USAF networks by:

- Not opening attachments or click on links unless the email is digitally signed, or directly verifying the source directly
- Not connecting any hardware or download any software, applications, music or information onto our networks without approval
- Encrypting sensitive but unclassified and/or mission critical information
- Installing the free Department of Defense anti-virus software on home computers⁷

As always, USAF Airmen are the core of our mission success; and the civilians and contract partners of the USAF also play a unique and critical role. Technical competence alone is not sufficient to meet the challenges of the 21st century. Airmen must be technically astute, tactically competent, armed with warrior ethos and equally prepared to deploy forward or operate in place to accomplish the mission. The USAF will increase cyber expertise by implementing a focused recruitment strategy, a specific and carefully managed cyber career pathway and career-long professional development.

The USAF will increase opportunities for education and provide specialized organic cyber operational training to include a centrally managed force of trained personnel with forensic and other specialized skills. The USAF will develop procedures to identify and track cyber professionals within the USAF personnel system and leverage the contributions of the Air National Guard and Air Force Reserve Command to develop and present unique capabilities.

The Specific Role and Training Methods of the 26 Network Operations Squadron

The 26 Network Operations Squadron

The 26 NOS is a vital part of the USAF cyberspace defense strategy. The squadron is part of the 24th Air Force, 67th Network Warfare Wing. The approximately 200-man 26 Network Operations Squadron located in Montgomery, Alabama was activated by Special Order GD-018 on 11 Aug 2009. The invaluable mission of the squadron is as follows:

The responsibilities of the 26 NOS are paramount to the successful operation of the USAF intranet. The 26 NOS operates the AF Enterprise computer network that consist of 16 Gateways and LAN equipment at over 250 locations that rely on over 600 WAN circuits supporting warfighting efforts for Operations IRAQI and ENDURING FREEDOM while executing 24/7 around the clock situational awareness and direction over the underlying network infrastructure and critical application operations. The squadron provides full service helpdesk for command and control and operational support network applications. The squadron also manages the AF authorized service interruption process to ensure minimal impact to sustaining base and deployed operations. 26 NOS directs the AF network security patch management process to ensure security of information riding on the AF networks. It also provides and monitors embedded implementation to detect network anomalies before mission impact to operations of all Air Force Active Duty, Air Force Reserve and Air National Guard classified/unclassified services.

The squadron pursues two- major avenues of training, Initial Qualification Training and Mission Qualification Training (MQT). Both are tailored to the specific outcome they represent.

The 26 NOS training program consists of requirements and programs directed by the Air Force by way of general and specific documentation. The primary referenced documents in this NOSI are the AFNOC NOD *Master Training Plan*, AFI 36-2201V1, *Training Development, Delivery*,

and Evaluation, AFI 36-2201V2, *Training Management*, AFI 36-2201V3, *Air Force Training Program on-the-job Training Administration*, and AFI 21-116, *Maintenance Management of Communication-Electronics*. Supporting documentation is also found in AFI 33-115V1, *Network Operations (NETOPS)*, AFI 33-115V2, *Licensing Network Users and Certifying Network Professional*, and 26NOGI 13-302V1, *Training Program*.

Initial Qualification Training (IQT)

IQT is mandatory for all new employees to the squadron, whether they are military, DoD civilian or contractor. All new hires report to the Training Manager after their initial on-day orientation on their first day of hire for the upcoming IQT schedule. During IQT, employees report to the Chief of Training and not to the Team Lead. After successfully completing the IQT, trainees are released back to their assigned Team Lead and begin MQT.

IQT addresses both administrative issues and technical concepts such as:

- USAF History and Customs
- Resource Protection
- Classified Handling
- Information Assurance
- Operational Security
- Safety
- Records Management
- Fraud, Waste and Abuse
- Secure Communications
- Office of Special Investigations
- Supply
- Customer Care
- Change Management
- AF Network Operations
- The 26 NOS Organization
- Information Operations
- Technical Orders
- Networking Fundamentals
- Network attack methods
- Defense in Depth
- CyberLaw
- Network applications and Access
- Site-specific applications
- RF/Emissions Security

An example of the coverage of one of these can be found in Appendix A. Upon completion of the five day course, the trainer and trainee sign the trainee as qualified on the Training Record. If the trainee or trainer feels the trainee is not qualified, then the instructor must schedule one-on-one time with the trainee.

At the conclusion of the five-day IQT and the signing of the Training Record, the new employee has seven days in which to take the Initial Qualification Exam. This exam is a 250 question assessment of their learning during the five-day period and is given by the Standards/Evaluation manager. A score of at least 85 is required. If the employee fails, then the employee must attend IQT again. If the employee fails the IQE again, then a meeting is set up with the Team Lead, Chief of Training, Standards Evaluation Manager and the Squadron Commander to address what action(s) need to be addressed.

Mission Qualification Training (MQT)

Trainees proceed to MQT immediately following completion of IQT and passing the IQE. MQT is completed NLT 6 months from the employee's orientation date. Team Leaders shall decide which tasks are applicable to the employee and load those blocks and tasks to the trainee. MQT is essentially on the job training held between the trainee and the Team Lead and other training personnel in the specific position field. For example, a new trainee might be assigned to be a router technician and so, over the next six months, learn the fundamentals of how this is performed in the 26 NOS. Two examples of this training can be found in Appendix B.

Trainers, Certifiers, Supervisors, and Team Leads document the Supervisor Record of Training (SRT) in the trainee's record for significant training actions. This is especially important for delays in training due to TDY, illness, etc.

The DoD requires maintenance technicians with privileged access to obtain and maintain the appropriate Information Assurance (IA) certification. If required, these certifications must be obtained within six months of employment (DAA may grant a six month waiver). Supervisors shall immediately notify new hires of this requirement and annotate the trainee's SRT of this notification. The trainee and the supervisor shall digitally sign the SRT.

Those individuals that do not meet DoD 8570 requirements, as specified in the contract, will not perform any maintenance actions on AF networks without a certified individual supervising the action.

If an individual does not obtain the required certifications within the allocated time will have all privileged accounts disabled.

Teams may break into duty positions for MQT purposes. Therefore an individual is deemed Fully Mission Qualified (FMQ) when finished with assigned MQT tasks. For example, the Firewall Team may break into a LAN and WAN. To be FMQ an individual only has to complete the tasks required for one position.

Upon receiving FMQ status, an employee may train and certify on other tasks associated with the respective team, outside the duty position. For example, a trainee receives FMQ status for the LAN duty position within the Firewall Team. The trainee then may train on WAN duty position tasks. However, a trainee may not train on Operations Team or System Administration tasks without meeting the requirements described in the 26 NOS Master Training Plan, Chapter IV.

Certification and all other requirements still apply when training into other duty positions.

Currency Training

Currency Training is required periodic training. This training may be directed by the Higher Headquarters, 26 NOS Commander, Site Lead, Chief of Training, MTM, Team Lead, or Shift Lead. Training intervals are determined by the individual or office requiring Currency Training. These are examples of currency training:

- Resource Protection
- Classified Handling
- Information Assurance
- Operational Security
- Safety

Currency Training is documented on the Recurring Training Document (RTD) in the employee's training record.

If a trainee is overdue on a task, the trainee is to complete the training immediately. Until the trainee meets currency requirements, the trainee may not perform the task without supervision, train or certify others on the task.

If a trainee is overdue on a task for more than 30 days, then the team trainer decertifies the trainee and annotates the SRT.

Conclusion

Cyberspace is a fairly new arena where both good and bad coexist. It can be argued that without cyberspace, information can no longer be effectively disseminated throughout the world. Yet, cyberspace is also rife with dangers. Effective training is one way to mitigate these dangers. Training is highly regarded in both the United States Air Force and the 26 Network Operations Squadron. It is only through the diligent and effective efforts of many qualified personnel that incoming personnel are properly trained so as to become proficient warfighters in the ever-changing cyberspace arena.

APPENDICES

APPENDIX A

Classified Handling Agenda

1. Identify and Explain Classified Handling Procedures
2. Identify and Explain Courier Procedures
 - a. Identify and Explain Packing and Wrapping Procedures
 - b. Identify and Explain Transporting Procedures
 - c. Identify and Explain Hand Receipting and Storage Procedures

3. Identify, Explain and Report Security Incidents
4. Identify, Explain and Report COMSEC Incidents
5. Identify Classified and Unclassified Information Categories
6. Identify and Explain Physical Security Requirements
7. Identify and Explain Safeguarding and Controlling Access
8. Identify and Explain Destroying Classified Information

APPENDIX B

TASK TRAINING GUIDE PART I				
BLOCK #: 202	MQT Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> X	IQT-A Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	IQT-T Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
BLOCK TITLE: PORTS, PROTOCOLS & FIREWALL CONFIGURATION	REV A	DATE 25 Sep 09	STAN/EVAL Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	TIME 25 Hours
COURSE CONTENT				
<p><u>EQUIPMENT</u></p> <p>Windows enabled SIPR computer with Monitor and Mouse Access to Lynx and Trigger servers</p> <p>And/Or</p> <p>Whiteboard with multi-colored markers</p> <p><u>VISUAL AIDS</u></p> <p>Port List Student Handouts Three-Way Handshake Handout Configuration Practice Worksheet</p> <p><u>REFERENCES</u></p> <p>Newton’s Telecom Dictionary, 17th Edition AnswersThatWork.Com</p> <p><u>CERTIFICATION REQUIREMENTS</u></p> <p>None</p>				

TASK BREAKDOWN

- *Define a Port
 - *Identify the common Ports and their Usage
 - *Define a Protocol
 - *Identify the common Protocols and their Usage
 - *Perform Firewall Configurations to Allow or Block Port and Protocol Traffic
- * Denotes a Critical Task

APPROVAL OF LESSON PLAN

	SIGNATURE	DATE
Training Manager		
Team Leader		
Site Leader		
Commander		

TASK TRAINING GUIDE PART II	
BLOCK #: 202	
BLOCK TITLE: PORTS, PROTOCOLS & FIREWALL CONFIGURATION	
COURSE CONTENT	
<p><u>TASK BREAKDOWN</u></p> <ul style="list-style-type: none"> • *Define a Port • *Identify the common Ports and their Usage • *Define a Protocol • *Identify the common protocols and their Usage 	<ul style="list-style-type: none"> • A logical interface between a process or program and a communications device or facility. *Ports range from 0 to 65,536 *Well known ports are 0 to 1023 and are assigned by IANA *Used in context with Transmission Control Protocol (TCP), TCP/IP and User Datagram Protocol (UDP). • Refer to Port List Student Handout *Discuss various other ports such as VOIP, VTC, etc that are not on the list* • A protocol is a specific set of rules, procedures or conventions relating to format and timing of data transmission between two devices. • Common Protocols 10. Internet Protocol (IP) – integral part of the TCP/IP suite 11. Transmission Control Protocol (TCP) – connection oriented, such as web 12. User Datagram Protocol (UDP) – protocol for sending messages or information without requiring a continuous connection 13. Three-Way Handshake

- Perform Firewall Configurations to Allow or Block Port and Protocol Traffic

- To properly allow or block traffic flow through a firewall, the syntax must be in correct order and without error.

14. Use the following flow chart to ensure correct configurations:

Action (Permit or Deny)–Protocol-
Source Host-Source Port-Destination
Host-Destination Port

Example #1 – Allow workstation IP 192.112.90.230 to a IP 198.118.80.9 for web server traffic

SYNTAX:

Permit tcp host 192.112.90.230 host
198.118.80.9 eq 80

Example #2 – Block the above web server IP from accessing the workstation IP via web port

SYNTAX:

Deny tcp host 198.118.80.9 host
192.112.90.230 eq 80

DISCUSS AND ANSWER QUESTIONS

*Provide Configuration Practice Worksheet for students to accomplish. Evaluate and discuss discrepancies.

*Denotes a Critical Task