

AIR WAR COLLEGE

AIR UNIVERSITY

Shaping the Air Force Operational Environment in Cyberspace

by

John C. Rogers, YC-03, DAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

12 February 2009

Distribution A: Approved for public release; distribution unlimited.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE MAR 2009		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Shaping the Air Force Operational Environment in Cyberspace				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air War College, Air university Maxwell Air Force Base, Alabama				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 39	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but it is the property of the United States government.

Table of Contents

Disclaimer	i
Table of Contents	ii
Table of Illustrations	iii
Biography	iv
Introduction	1
Historical Background	4
“World Wide Web” An Open Environment	6
Provisional Cyber Command.....	7
Current Air Force Supporting Role.....	8
Defining Air Force Cyberspace Requirements	9
Define the Mission Requirements.....	10
Cyberspace Doctrine and Strategic Defense Strategy	11
Shaping an Air Force Cloud	12
Design a Defensive Cloud	13
Develop a Cyber Workforce	15
Create a New Mindset.....	19
Air Force Cloud Implementation Plan	20
Step 1 - Build the Team and Set Priorities.....	21
Step 2 - Build Security into System Engineering and Architecture.....	22
Step 3 - Build Organic Core Infrastructure for new Cloud.....	23
Step 4 - Build Application Security throughout Lifecycle	25
Step 5 - Build Operations Security	26
Summary	27
Bibliography	29
Appendix A	34

Table of Illustrations

Figure 1 OSI Reference Model	14
Figure 2 Pipeline of Declared CS Majors (Supplied by CRA Taulbee Survey).....	17
Figure 3 System Design Process.....	22
Figure 4 New Gateway Configuration	23
Figure 5 Building in Security during Entire Project (Supplied by Fortify)	25

Biography

Mr. John C. Rogers is currently a student at the Air War College at Maxwell Air Force Base, Alabama. His permanent civilian position is as Director, Information Assurance Directorate, Air Force Communications Agency. Mr. Rogers retired from the active duty Air Force in 1999 after spending over 20 years of honorable service in the aircraft/communications career fields. He has been a DAF civilian employee since November 2000. During his time as a civilian, he has served as the Chief Engineer with the Air Technology Network, filling the roles of Technical Team Leader and Resource Advisor, providing technical solutions for installing and maintaining a worldwide network of over 86 downlinks and 5 uplinks. He has worked at both the wing level, as wing Information Assurance officer, and base level, in the communication squadron SCB flight. Mr. Rogers served as the Certification and Accreditation Branch Chief and Policy Support Division Chief in the Air Force Communications Agency where he directed the integration of systems into the Air Force network to achieve integrated and interoperable Air Force CONOPS capabilities.

Mr. Rogers holds a Masters of Science in Education from the University of Maryland as well as a Bachelors of Science in Aeronautics from Embry-Riddle Aeronautical University where he graduated Summa-Cum-Laude. He has been awarded the Meritorious Civilian Service Medal and the Exemplary Civilian Service Medal. Mr. Rogers has also been awarded his certification as a Certified Information Systems Security Professional (CISSP), one of the highest civilian certifications within his field. Mr. Rogers is a life member of the Armed Forces Communications and Electronics Association and Past-President of the Federal Government Distance Learning Association where he received the coveted "Pioneer Award."

Introduction

The Air Force is losing the battle to defend cyberspace and each day the United States faces increasing threats and attacks against its networks aimed at the theft, manipulation, or destruction of information. The loss of information caused by inadequate cyber security has inflicted unacceptable and often incalculable damage to US national and economic security interests.¹ The Air Force has dedicated considerable resources trying to manage and secure information and information systems in cyberspace. Air Force personnel have tried to create a number of secure operational environments in the cyberspace domain, all based on technology developed in the 1950s and 1960s for an open, highly fragmented, system centric, architectural environment. One major problem with this approach is that the Air Force frequently fields systems and applications that are often outdated upon implementation and susceptible to attack in that open environment. Another problem with this approach is that the infrastructure used to create the current environment was, in most cases, commercial off the shelf (COTS) products, designed and built by our adversaries. Instead of this approach, the Air Force could redefine what is meant by an “Air Force Operational Environment” and move to a more cloud centric approach where the priorities are set by the cloud and not by applications or individual needs. The Air Force should develop the doctrine, strategies, applications, and infrastructure necessary to create, defend, and dominate its own “Air Force Cloud.”

Implementation of an Air Force Cloud will affect the operational environment which includes the six phases of the kill chain process (find, fix, track, target, engage, and assess). The systems that provide war fighters with the capability to execute the kill chain are connected by a common thread, cyberspace via the cyber network. One of the objectives should be to reduce the

¹ Lewis, James A., “Securing Cyberspace for the 44th Presidency”. *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Center for Strategic and International Studies, Washington, DC, December 2008.

latency in the kill chain in a contested cyber environment where US dominance has not been established. Regrettably, the Scientific Advisory Board 2008 Cyber Study concluded that the Air Force mission is at risk and that the Air Force is not ready to operate in a contested cyberspace environment. The Air Force must change its fundamental philosophy concerning cyberspace and overcome its challenges by achieving true integration, interoperability, and epistemological reliability in its networks.

The Joint Chiefs of Staff defines “cyberspace” as a “domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical structures.”² This definition makes no mention of the internet, intranet, Non-secure Internet Protocol Router Network (NIPRNet), or Secure Internet Protocol Router Network (SIPRNet) which comprise some of the terms most often associated with cyberspace. Deputy Secretary of Defense, Gordon England, later defined cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”³ There is now a distinction between the domain and manipulation of that domain by people and technology. With seemingly unlimited technologies and methodologies available to manipulate the environment to meet operational requirements, the Air Force is limited only by the skills and imagination of its personnel and its willingness to focus resources in this area. Exactly how that is done by the Air Force is the foundation of this research, leading to identifying an effective way for the Air Force to shape a segment of the cyberspace environment in such a way to ensure epistemological reliability while fulfilling its war fighting mission. Three basic research

² Joint Publication (JP) 3-13, *Information Operations*, 13 February 2006.

³ England, Gordon. "The Definition of "Cyberspace." Dep SECDEF Memorandum to Secretaries of Military Departments, et al., 12 May 2008.

questions are: 1) What portion of the cyberspace domain must the Air Force design and build to successfully conduct its core operations? 2) What is the best way to shape that segment of the cyberspace domain to conduct those operations? And, 3) How can the Air Force implement this new Cloud?

This paper will provide provocative answers to these three research questions. It will start by examining the historical evolution of roles the Air Force has played in the cyberspace domain and some of the challenges created along the way. It will look at the early days of the “World Wide Web” and later efforts by the Air Force to stand up a Cyber Command. The paper will also examine recent policy changes at the Department of Defense (DoD) that have reestablished the Air Force organize, train, and equip (OT&E) role with respect to presenting forces and capabilities to the Combatant Commands for cyberspace operations and the challenges it still faces with operating and defending its own networks. The paper will identify doctrinal and strategic changes that will have to take place to implement an Air Force network to meet its OT&E requirements in a secure environment. It will answer the question of how to shape a secure operating environment and the resources and workforce required to make that concept a reality. Lastly, the paper will present a five-step plan for successfully building a defense-based Air Force Cloud. This plan will include: 1) Building the team; 2) Building security and survivability into the basic system engineering and architectural design of the Cloud; 3) Replacing core infrastructure with technology based on the new Cloud concept; 4) Designing security to be baked-in to applications in the development process and not bolted on later; 5) Instituting operational security by designing processes and systems that can survive in a contested cyber environment and which are self-healing in order to better recover from

damage/attacks. In order to understand how to move forward, the Air Force must first look at its earliest beginning in cyberspace.

Historical Background

As the processing power of computers continues to grow at an exponential rate, the amount of information which can be stored and processed by these machines is also increasing. In the beginning, most of these machines were in a standalone configuration and the information had to be physically brought to the computer to be processed. Built in 1946, ENIAC is often considered the first supercomputer; it used around 20,000 vacuum tubes and weighed over 30 tons, taking up a tremendous amount of floor space and consuming almost 200 kilowatts of electrical power.⁴ The ENIAC led the computer field during the period from about 1949 through 1952 when it served as the main computational workhorse for the nation's scientific problems.⁵ As was typical of the time, the Air Force often housed its computers in what was referred to as a block house, which was a large building with no windows. The block house usually required one floor for the cooling equipment, one for all the tubes, one for the peripheral devices, and one for personnel. Programs and data were inputted through devices called card readers which often took six to eight hours to process a single stack of cards at a rate of about 150 cards per minute. Then in 1958, the Seymour Cray's CDC 1604, the first in a series of Cray computers, was built as a fully transistorized supercomputer.⁶ As machine capabilities continued to grow and the value of the data stored in them began to be realized, the need to share this data became evident. As has often been the case with advances in technology, the military, through the Rand Corporation,

⁴ Weik, Martin H., *The ENIAC Story*, Ordinance Ballistic Research Laboratories, Aberdeen Proving Ground, Maryland, 1961.

⁵ Weik, Martin H., *The ENIAC Story*, Ordinance Ballistic Research Laboratories, Aberdeen Proving Ground, Maryland, 1961,

⁶ Calle, Dan, CS 3604 Assignment, *Supercomputers*, Spring 1997,

began to fund research to find a way to connect those individual computers so they could share their data.

It could be argued that cyberspace came into existence sometime around 1969 when the Advanced Research Projects Agency (ARPA), later designated DARPA, first established the ARPA Network (ARPANet), a small network linking four similar mainframes at four different sites. In 1972, Robert Kahn and Vinton Cerf released their paper on a new internet protocol (IP) that would allow incompatible networks to talk with each other on a much larger scale.⁷ This new protocol would act as an interface among networks to transmit data in such a way as to allow any application to run over it layered on top of any physical network. By 1975, ARPANet had matured enough and grown to a point that DARPA turned it over to the Defense Communications Agency, known today as DISA, to manage. A new protocol TCP/IP was successfully used in 1977 to link four networks together and in 1983, the ARPANet formally migrated to TCP/IP, also known as internet protocol version 4 or IPv4, and morphed into what is known as the “Internet” today.⁸ The introduction of IPv4 might be considered the first true instantiation of cyberspace as we know it today with the term World Wide Web appearing later when browsers, such as Mosaic and Navigator, became common. Around that same time, an unclassified military-only network split off from the ARPANet to conduct operations in a closed network without “outsiders” viewing the information. Called the Military Network, it remained connected only at a small number of gateways for exchange of electronic mail that could be easily disconnected for security reasons if required, eventually becoming part of the DISA

⁷ ARPANET 1970s, Cyberte telecom Federal Internet Law and Policy

⁸ ARPANET 1970s, Cyberte telecom Federal Internet Law and Policy

Defense Data Network (DDN).⁹ The DDN was replaced in 1995 by the NIPRNet, SIPRNet, and the Joint Worldwide Intelligence Communications System, all of which are still in use today.¹⁰

“World Wide Web” an Open Environment

Wikipedia defines the World Wide Web, commonly shortened to the Web, as a system of interlinked hypertext documents accessed via the Internet. The World Wide Web was created in 1989 by English scientist Tim Berners-Lee, working at the European Organization for Nuclear Research (CERN) where he built all the tools necessary for a working Web: the HyperText Transfer Protocol (HTTP), the HyperText Markup Language (HTML), the first Web browser, the first HTTP server software (later known as CERN httpd), the first web server (<http://info.cern.ch>) and the first Web pages that described the project itself.¹¹ In February 1993, the National Center for Supercomputing Applications, at the University of Illinois at Urbana-Champaign, released the first version of Mosaic, which was to make the Web available to people using PCs and Apple Macintoshes, and the rest is Web history.¹²

Since that time, the use of the Web has grown to a point that many people would find it hard to function without it. This access to vast amount of data and information which traverses the electrons of the Web has substantially increased the speed and efficiency with which most people are able to complete their job; this is also true of the military. It is the very nature of this instantaneous access which also presents a number of problems associated with security and privacy of the information involved. Security firm BitDefender highlighted mobile malware, botnets, phishing, and identity theft as the main internet threats for 2008 and predicts an increase in targeted exploits of malware and money-driven actions, attempts to collect private databases,

⁹ ARPANET 1970s, Cybertelexcom Federal Internet Law and Policy

¹⁰ Grant, Rebecca. *Victory in Cyberspace*. Arlington, VA, Air Force Association, 2007

¹¹ http://en.wikipedia.org/wiki/History_of_the_World_Wide_Web

¹² <http://info.cern.ch/>

financial information and internet banking details.¹³ The open architectural nature of the web makes it extremely difficult to find the perpetrators and, if found, prosecute them due to legal limitations. Most laws today are based on physical boundaries such as state and international borders, none of which are relevant in cyberspace. Anyone who has a computer and access to the Web can become a participant or troublemaker to the orderly flow of information, much like the rule of law in the days of the Wild West. The world will eventually have to realize that if the web is to be a viable medium with which to conduct business, enforceable limitations on its use will have to be imposed and boundaries established or it will remain the domain of outlaws and it will be considered the “Wild Wild Web” with little or no controls or boundaries.

Provisional Cyber Command

Understanding the need to control and dominate the cyber environment during military actions, the Air Force set plans into motion to develop an organization called Cyber Command. Towards that goal, the Air Force officially stood up a provisional Cyber Command on September 18, 2007. A provisional unit is a temporary unit organized to perform a specific task and is considered temporary because it does not have personnel assigned; personnel are attached to the unit from their home stations.¹⁴ Major General William Lord, Chief of Air Force provisional Cyber Command, gave his new troops a fairly narrow charge: better operation of the Air Force's networks saying "It's about the Air Force's focus on the Air Force's protection and defense of the Air Force's command and control capabilities."¹⁵ His direction excluded computer network attack and computer network exploitation from the mission set of the provisional command. The logic behind this approach is that the Air Force must be able to secure and defend its networks before engaging in attacks on, or exploitation of, opponent's networks. The next step for the Air

¹³ James, Clement. *The Main Internet Threats for 2008*, 24 December 2007

¹⁴ Air Force Cyber Command (Provisional), *Concept of Cyber Warfare*, 26 November 2007

¹⁵ Shachtman, Noah, “Air Force Wobbles on Plan for Cyber Dominance.” *Wired - Danger Room*. 19 June 2008.

Force was the activation of Cyber Command, scheduled to occur one year after the activation of the provisional command, giving the Air Force the time needed to put all the pieces in place for an operational command. Before this could happen, questions began to surface about whether or not it was the Air Force's mission to fly and fight in cyberspace.

Current Air Force Supporting Role

General Moseley, then Air Force Chief of Staff, released a new mission statement for the Air Force on December 7, 2005 which stated "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."¹⁶ Adding cyberspace to the mission of the Air Force created a great deal of discussion within the DoD. Should responsibility for that mission be placed in the Air Force, another component, a combatant command, the DoD, or an agency outside the DoD? Secretary of Defense Robert Gates addressed this issue in a memorandum he released on November 12, 2008, addressing command and control for the military cyberspace mission (Appendix A). In that memorandum, he stated that there is a pressing need to ensure a single command structure is empowered to plan, execute, and integrate the full range of military cyberspace missions and that function will be under the operational control of the Director of the National Security Agency (NSA) in his role as the Joint Forces Combatant Commander for Network Warfare (JFCC-NW) under United States Strategic Command (STRATCOM).¹⁷ Under this new guidance, it is apparent that the Air Force role is not to fly, fight, and win in cyberspace, that responsibility has transferred to NSA as the JFCC-NW and it would seem the Air Force will once again have to adjust its mission statement to accommodate this new role. The Air Force now must assume a supporting role to OT&E forces for the fight and then be ready to present

¹⁶ Gettle, Mitch, MSgt, USAF, Air Force Releases New Mission Statement, Air Force Link, 8 December 2005

¹⁷ Gates, Robert M., Secretary of Defense "SECDEF Memo C2 for Military Cyberspace Missions". Nov 08

those forces to the combatant command when requested, mirroring the Air Force missions for air and space. Key to accomplishing this is the ability to design and deploy a network, or Air Force Cloud, for the OT&E mission with adequate defenses to ensure its survivability/usability during cyber attacks. Before the Air Force can design a Cloud, it must develop the doctrine and strategy to be followed during the design and operation of that Cloud.

Defining Air Force Cyberspace Requirements

Until now, the Air Force has been operating in the cyberspace domain in an environment that was developed without having its core mission as the driving force behind that development. This is in direct conflict with military theorists like Sun Tzu and Clausewitz. Sun Tzu expressed this most appropriately, when he stated, “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”¹⁸ The core equipment and technologies, which comprise the foundation of the current environment, have been increasingly developed by individuals, corporations, and nation states that do not have the US domination of that domain as their priority. This is highlighted by the recent newspaper reports of requests from other nations for the domain name servers to be moved outside the United States and out from under US operational control. The speed of growth, increased reliance, and uncertainty of the cyberspace domain has created a dilemma for the Air Force. How should the Air Force respond? The Air Force must get back to basics and apply the same strategies and doctrine to the cyberspace domain which are applied to air, land, space, and sea domains.

¹⁸ Sawyer, Ralph D., “Sun TZU – Art of War”. Westview Press Inc, Boulder Colorado, 1994

Define the Mission Requirements

The first step in shaping this new operational environment is to define the requirements and capabilities an independent Air Force Cloud would have to provide to the Air Force and Combatant Commanders. Obviously, it must be an enabler for the accomplishment of the Air Force OT&E mission for air, space, and cyberspace. The Air Force must also be able to extend, field, and support an expeditionary capability of that Cloud for the combatant commander. It is then necessary to identify those critical requirements unique to the Air Force, such as the reliable delivery of the Air Tasking Order, and the capabilities necessary to successfully meet those requirements. This will require a fundamental shift in culture and ideology from an offensive to a defensive mindset. Secretary Wynne would argue that in this context, defensive operations not only refer to information assurance and survivability of the network, but also to protecting the ability to conduct offensive operations, if necessary.¹⁹ This view purports that part of the Air Force OT&E mission is to prepare cyber warriors to conduct both offensive and defensive operations in a contested cyber environment.

Inherent in that thought is the fact that, to train cyber warriors, the Air Force must have a cyberspace environment to conduct that training. That does not mean that the actual internet as we know it today needs to be used for that purpose. Just as the military uses simulators and test ranges to train for the air, land, and sea missions, a simulator or test range could be established to train cyber warriors as well. If there is to be an offensive capability within the cyber warrior skill-set, the Air Force Cloud must also include connectivity to the rest of cyberspace for the warrior to conduct his or her specialty. Combined, these highlight the requirement for an Air Force Cloud capable of meeting the OT&E requirements for air, space, and cyberspace,

¹⁹ Wynne, Michael W. Secretary of the Air Force. "Flying and Fighting in Cyberspace". *Air and Space Power Journal* 21, Spring 2007

defensible against our adversaries, expeditionary in nature, providing secure connectivity to the rest of cyberspace, and providing a training environment for future cyber warriors. With this as a foundation for an Air Force Cloud cyberspace mission, it is necessary to develop doctrine and a strategic view on how it should be utilized.

Cyberspace Doctrine and Strategic Defense Strategy

A precursory look at AFDD 2, dated April 3, 2007, provides 25 foundational Air Force doctrine statements that are basic principles and beliefs upon which other AFDDs are built, none of which mention cyberspace.²⁰ Most could simply be adjusted from reading air and space to reading air, space, and cyberspace. Others would have to incur greater modification to accommodate this new domain. It would also be necessary to add a statement such as “Cyberspace superiority is the desired state before all other combat operations. Attaining cyberspace superiority provides both the freedom to attack and freedom from attack, as well as ensuring freedom to maneuver. Operating without cyberspace superiority radically increases risk to surface and air operations,” to the list to make it complete. This statement, much like it did for air power, highlights the importance of gaining cyberspace superiority in the battles of tomorrow. Just as air power increased the speed at which effects could be delivered, cyberspace now makes it possible to deliver effects in nanoseconds rather than minutes or hours.

One of the greatest effects which cyberspace brings to the battlefield environment today is as an enabler of technology, enhancing the capabilities of air, land, sea, and space operations. As a result of this, all of the other domains have grown increasingly dependent on the information and links utilized through the cyber domain to complete their mission. This means the epistemological reliability of the cyber domain must be assured before engaging the

²⁰ Air Force Doctrine Document (AFDD) 2, *Operations and Organization*, 3 April 2007

adversary in those domains. The Air Force is working diligently to publish a doctrinal document associated with cyberspace in the form of AFDD 2-11, Cyberspace Operations, but only drafts have surfaced to date. This effort must be accompanied by a new strategy to effectively and efficiently develop and utilize the cyberspace domain and the capabilities it brings to the table.

The United States National Strategy to Secure Cyberspace lists three objectives: preventing cyber attacks against critical infrastructure; reducing vulnerability to cyber attack; and minimizing damage and recovery time once attacked.²¹ The objectives for the defense of the United States cyberspace environment provide an excellent foundation for developing a strategic defense strategy for operation of the Air Force Cloud. In addition, the Air Force strategy should include the ability to ensure Air Force cyber warriors the operational freedom of action within the Air Force Cloud while denying adversaries the ability to do the same. Once these requirements can be met, there must be an expeditionary capability to take the fight to the enemy and provide effects-based operations as required by the combatant commander. All of the items listed above point to the development of an Air Force Cloud built with defensive capabilities in mind with a premium on survivability and operability in a contested cyberspace environment. What remains is the task of shaping the Air Force operational environment to meet the requirements identified above.

Shaping an Air Force Cloud

The Air Force must reverse many of the trends it has established over the last 15 years if it wants to establish an Air Force Cloud as described above. Cyberspace will have to be looked at as a domain that does not belong to the Air Force. Rather, the Air Force must be able to establish, within cyberspace, an area it can establish, control, and conduct offensive and

²¹ Air Force Cyber Command (Provisional), *Concept of Cyber Warfare*, 26 November 2007

defensive operations. There must be limitations on the utilization of that space and the Air Force must develop the organic capability to establish, control, and fight within that domain with relying on outside sources to do so. Much of the Air Force effort today is focused on offensive operations, probably due to the intrinsic war fighting nature of such operations within the domain. This will have to change and efforts shifted to first establishing a secure domain, developed and operated by competent warriors capable of establishing and delivering effects in that domain. The changes identified above are more than just surface changes, these changes will involve changing the very infrastructure, software, and systems, as well as the way they are developed and deployed in the cyberspace domain. The first step in this process is establishing a defensive-based Air Force Cloud capable of surviving in a contested cyberspace environment.

Design a Defensive Cloud

The current Air Force global information grid (AFGIG) is based on an open architectural environment which inherently favors offensive actions. For the most part, it was built with parts and software provided by industry partners who may or may not have Air Force security interest as a top priority. Recent events with both hardware and software suppliers from other nation states have shown how vulnerable our dependence on others to produce these products has made the Air Force. It would be impossible to shut down the AFGIG in today's operational environment and start over without adversely affecting the mission of the Air Force. Instead, the Air Force must begin to deploy a new AF Cloud, designed with defensive capabilities as its foundation and built with government designed or government off-the-shelf products. The most critical assets and data could be moved to the new Cloud immediately, followed by less sensitive or critical requirements. The design of the Air Force Cloud will be critical to being able to successfully migrate data and applications into it to ensure their security.

There are a number of ways to design the Air Force Cloud in such a way as to avoid the threats of intrusion or render them incapable of causing effects within the cloud. For these actions to be effective they must be implemented at the physical, network, and transport layers of the OSI model in figure 1. At the physical layer, the Air Force should build its own connectivity without utilizing commercial circuits and equipment. The Air Force must develop an organic capability to produce the equipment and programming necessary to ensure its reliability and security. At the network layer, the Air Force could develop a new protocol stack specifically for use by the DoD based on sessions rather than the packets currently utilized by TCP/IP. As discussed earlier, the current IPv4

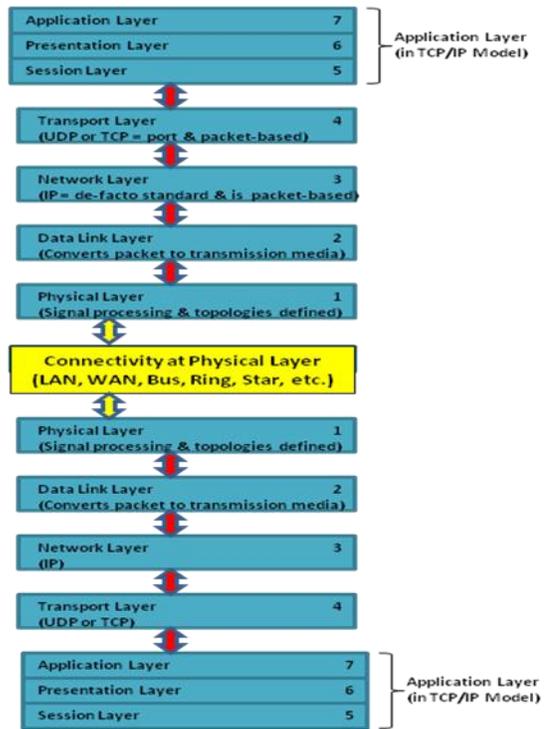


Figure 1 OSI Reference Model

protocol was implemented in 1983 and is considered an outdated and unsecure protocol. The military would have the option of developing its own protocol, maybe an IPgov in which various security features like IP security and geo-location could be built in and shared across the federal government, while still maintaining a linking capability with both IPv4 and the newer IPv6 (not yet widely used). Another option would be to hide all of our assets other than the gateway equipment behind a network address translation (NAT) and proxy schema. At the transport layer, error-free transmission requirements, as well as end-to-end user authentication, can be written into the session-based protocol used. An example might be using Session Initiation Protocol (SIP) which is designed to address the functions of signaling and session management within multimedia communications. All of these options, and more, will be discussed in greater

detail during the implementation plan section of this paper. Only when the new Air Force Cloud is operational can the Air Force begin to migrate its information and applications, starting with its most critical and sensitive assets. In order to successfully do that, the Air Force must have a qualified workforce capable of operating and maintaining its new Cloud.

Develop a Cyber Workforce

Air Force Chief of Staff, General Michael Mosley, tasked the service to “Provide combat ready forces trained and equipped to conduct sustained offensive and defensive operations in cyberspace.”²² The Air Force is trying to resolve this particular problem, although it has a long way to go to make up for some of the issues caused by previous budget cuts and downsizing efforts. In April 2008, the Secretary of the Air Force signed “The Air Force Roadmap for the Development of Cyberspace Professionals 2008-2018,” creating a long-term vision for cyber warriors.²³ This document grants authority for the development of 17D and 1BXXX Air Force Specialty Codes (AFSCs), identifies concepts of how to develop future cyberspace forces, and calls for the creation of a new Cyber Technical Center of Excellence to synergize efforts in the cyber domain. This effectively creates two well-defined areas within the new AFSCs: cyber operations for the 17D, 1B0, 1B3, and 1B4 AFSC’s and cyber systems and maintenance for the 1B1 AFSC.

The current plan is to provide training to the cyber operations AFSCs to prepare them to conduct cyber operations.²⁴ Based on this plan, the 17D, 1B3, and 1B4 would first attend undergraduate Cyber Warfare training consisting of a little academics and a lot of hands-on exercises and scenarios, operationally focused where officer and enlisted operators share

²² Jabboore, Kamal, Dr., “IA + THE SCIENCE & TECHNOLOGY OF CYBER WARFARE”, PowerPoint briefing for Air War College IO Seminar, 4 Sep 2008

²³ Hall, Bill, Col, USAF.”Force Development for Cyber Transformations”. PowerPoint briefing for Air Staff, Oct 2008

²⁴ Hall, Bill, Col, USAF.”Force Development for Cyber Transformations”. PowerPoint briefing for Air Staff, Oct 2008

common core training and split out to appropriate tracks.²⁵ This is a point which could be considered problematic since you could have enlisted personnel who are trying to employ air power doctrine with no training in that area. A recent speaker at Air War College also presented another problem with enlisted personnel filling these positions. In the joint environment they are often not taken seriously by field commanders; some do not even get a seat at the discussion table. In this respect, it is important that our cyber warfare operators, both offensive and defensive, be filled with military officers familiar with the application of air power and who have the authority to execute the commander's intent.

The 2008 AF/A3O Roadmap for Developing Cyber Professionals states that the Air Force will produce professional Airmen with the ability to establish, control, and leverage the cyberspace domain. It discusses the development of a Cyberspace Warfare Officer (CWO) 17D career field and then details how current 33S and 12X career fields will be converted to meet those needs. This is the wrong approach; it does not provide a true CWO classification capable of fulfilling the Air Force's needs. Currently, a 33S officer can hold almost any degree, including those unrelated to computers. A college-level algebra class does not provide the foundation necessary to perform the tasks required to establish, control, and leverage the cyberspace domain. This approach only focuses on operations within an already established domain and does not provide an answer for the need to establish the domain. There should be a minimum of two specialties within the CWO career field, a 17B and a 17D. One with the skills necessary to establish and control the cyberspace domain and the other capable of leveraging that domain through offensive and defensive operations. Each of these specialties should have a unique set of requirements necessary for entry.

²⁵ Hall, Bill, Col, USAF."Force Development for Cyber Transformations". PowerPoint briefing for Air Staff, Oct 2008

All CWO 17B officers should be required to have a computer programming or electrical/computer engineering degree. They should also be provided specialized training to equip them with the necessary tools to establish and control the new Air Force Cloud. All CWO 17D officers should be required to have a computer engineering or computer science degree. They should also be provided specialized Air Force cyber training to equip them with the skills necessary to leverage the cyberspace domain by conducting offensive and defensive military operations in cyberspace. While this would require a substantial investment, it is the only way to provide educated and trained combat forces capable of fighting in the cyberspace domain. CWO 17B and 17D career fields, independent of the 33S career field, should be established.

The establishment of a new Air Force career field, with the requisite education and training programs, could take years to accomplish.

Complicating matters is the decline of available civilian sector computer science candidates for entry into a CWO training pipeline (see Figure 2). To overcome this challenge, the Air Force should consider leveraging the Air Force Institute of Technology undergraduate program along with programs like

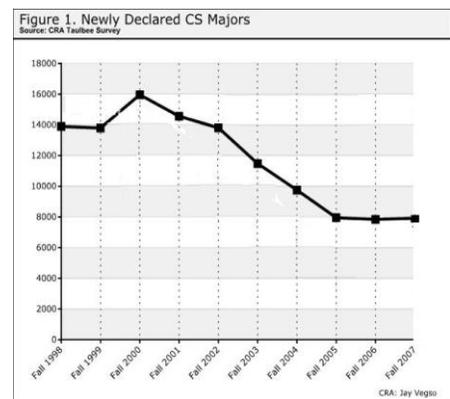


Figure 2 Pipeline of Declared CS Majors

the Advanced Course in Engineering (ACE) Cyber Security Bootcamp at Rome Labs to expand the pool of eligible candidates for the CWO 17B and 17D career fields. The ACE program focuses on future cyber warfare through technology-driven tactical cyber offense, threat-driven operational cyber defense, and policy-driven strategic effects based on commander's intent. This program could be used to develop the requirements and foundational courses for undergraduate cyber training similar in nature to the current undergraduate pilot training program. Simulators,

such as Black Demon and Bullwork Defender, could be utilized to provide realistic cyberspace training involving current military objectives and rules of engagement.

Attracting and retaining cyber warriors capable of operating in and dominating a contested cyberspace environment will take careful planning on the part of the Air Force personnel system. It must develop a realistic career path capable of providing advancement opportunities for the CWO 17B and 17D officers at all levels within the chain of command. This career path must include active duty service commitments for each level of progression along the path to ensure the Air Force can reap the benefits of these efforts. This process should also include DoD civilians of equivalent grades capable of providing continuity during the transitional and deployment periods often experienced by active duty officers. The backside of this process must include incentives of sufficient value to retain these highly trained cyber warriors. The Air Force cannot afford to expend time and resources to educate and train these individuals only to have them exit the service for civilian sector jobs which offer higher pay and better incentives. The personnel system must look at these individuals as an investment in its future, an investment which can provide great dividends in the long run if managed correctly.

With the 1B1 AFSC, the Air Force has done a great job at identifying core requirements, developing new career fields, and a career path for future cyber system maintainers. Each new cyber maintainer will receive a “Cyber Fundamentals” course similar to current maintainers receiving Electronic Principles before progressing on to their core courses to learn their specific AFSC.²⁶ In addition to these courses, the Air Force should consider providing supplemental and advanced cyber warrior courses to ensure its Airmen have the latest skill sets available and are proficient in applying those skills. Additionally, more work needs to be done in identifying facilities and instructors to provide the new cyber training, where these AFSCs will fit within the

²⁶ Cyber Enlisted Transformation Brief, Sep 2008

current Air Force organizational structure, and the number of each AFSC which will be required to accomplish its assigned mission, not to mention the support structure required for such a large-scale change in deployment capabilities. The current landscape will look completely different and the way it is conceptualized by the workforce will have to change also.

Create a New Mindset

Changing the parochial attitude of the Air Force as it relates to cyberspace and the mission it will perform in that environment will take both time and effort on the part of senior leaders. Defensive cyber operations are vital to protecting, preserving, recovering, and reconstituting cyber related capabilities before, during, and after an adversary attack.²⁷ Like air and space, cyberspace is unrestricted by boundaries and has the ability to extend the battlefield to the US homeland. It has also become a great enabler for other warfighting capabilities employed in the other domains. For these reasons, it is extremely important to protect the Air Force's ability to effectively utilize cyberspace in its application of force. This is a paradigm shift from the inherently offensive nature of air operations and the glamour associated with computer network attack. It will also take a considerable amount of new technology, increased budget expenditures, and a greater reliance on internal development to ensure the reliability of an Air Force Cloud. Change of this type will require a review of all of the IT assets and systems within the Air Force and conscious effort to develop a prioritized list based on mission requirements.

An organization as large as the Air Force is unlikely to change overnight. It will take time to develop some of the hardware and software necessary to implement the changes listed above, as well as to educate and train future cyber warriors for the tasks that lie ahead. There will be an interim period where both the AFGIG and the new Air Force Cloud will be utilized.

²⁷ Air Force Cyber Command. *Concept of Operations*, Draft version 4, 21 December 2006

During this period, legacy systems can be evaluated for relevancy and currency of application and decisions can be made on whether to migrate them to the new cloud or to develop new applications for those processes within the new Cloud. Just as with other changes, this process must be undertaken in a series of steps, each building upon the other until the process is complete. It is important to identify the steps prior to implementation to ensure that all involved in, or affected by the change, have an opportunity to have an input into the plan.

Air Force Cloud Implementation Plan

Unfortunately, the message about the real cyber threats and the steps necessary to avoid or prevent them is not getting the traction it deserves within the Air Force. Dr. Kamal Jabbour, senior scientist at Rome Labs and a key participant in the 2008 Scientific Advisory Board Cyber Study, stated that the Air Force is not ready to operate in a contested cyber environment, putting the Air Force mission at risk. A lack of focus by the Air Force on the development of cyber forces and capabilities has also hindered the service's presentation of these key enablers to the joint warfighter.²⁸ This conclusion highlights the first step necessary in implementing a plan for building an Air Force Cloud; assembling the team of professionals capable of establishing the new Air Force Cloud and setting priorities for the events necessary to do so. It will also take a considerable amount of new technology, increased budget expenditures, and a greater reliance on internal development to ensure the reliability of an Air Force Cloud. Change of this type will require a team effort, a review of all of the IT assets and systems within the Air Force, and a conscious effort to develop a prioritized list based on mission requirements.

²⁸ Wynne, Michael W. Secretary of the Air Force. "Flying and Fighting in Cyberspace". *Air and Space Power Journal* 21, Spring 2007

Step 1 - Build the Team and Set Priorities

Making the changes identified above will encounter substantial resistance from many of the AFGIG operators today who believe they are adequately protecting Air Force assets with the systems in place today. Establishing a team to champion the effort to establish a new Air Force Cloud is key to creating a foundation for success. The team must be composed of qualified individuals who understand and support the need for change in this area. This team must be capable of thinking outside the box and designing a Cloud built with organic assets capable of implementing the commander's intent at cyber speeds. There are a number of organizations whose participation as part of this team is essential: DoD, Rome Labs, AFCA, ACC, AFSPACE, AFNETOPS, GCIC, STRATCOM, and others. The first task for the team will be to identify all of the cyber assets currently in the Air Force inventory and develop a prioritization process for the assets related to mission needs.

Every asset in the Air Force inventory can be categorized according to its critical nature in the accomplishment of the mission. Command and control systems would be high on the list of critical systems during a conflict. The Air Force must begin the process of identifying and prioritizing its IT assets, determining which are critical to the mission and which are nice to have. This same process must also be applied to the information stored and transmitted across those systems as the components within a system such as the processor, memory, or peripheral devices. The real questions become: what items is the Air Force willing to risk being without during a cyber war? What information is it willing to lose or do without? Risk can be defined as a function of the likelihood of a given threat exercising a particular potential vulnerability.”²⁹ This means the Air Force defensive efforts will go to ensuring the survivability of its most

²⁹ NIST Publication SP 800-30: Risk Management Guide for Information Technology Systems, July 2002

critical assets first before all else. As an example, a core router in the conflict area would be more critical than at an individual desktop at a stateside base. Once all of the assets have been prioritized, designing architecture to support those requirements and engineering the systems necessary to meet those requirements in the new Cloud is the next step.

Step 2 - Build Security into System Engineering and Architecture

Confidentiality, integrity, authentication, attribution, and availability are system properties that must be built in during the systems engineering process and during system-of-systems design. The later in the system lifecycle development process that security is added, the greater the cost of doing so will be and the probability of getting things right the first time decreases. It is important to have a process that continually assesses the information protection and security measures throughout the engineering and architectural process. Figure 3 shows a six-step process that continually assesses information protection effectiveness and heavily involves the user from start to finish.

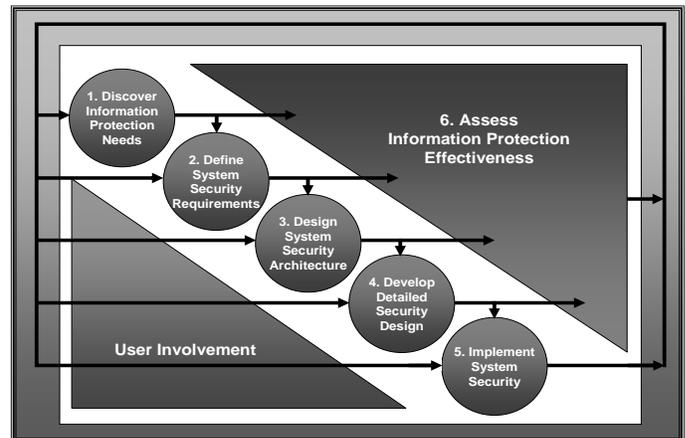


Figure 3 System Design Process

The process includes identifying information protection needs at the beginning and using that to define what security requirements will be necessary to ensure those needs are met. Only after these issues have been addressed can the architectural and engineering process take place, each with a link to user and security to ensure their needs are still being met. Even as one enters the implementation stage of the process, there are checks to make sure that security has not been compromised and the user's needs are being met.

Step 3 - Build Organic Core Infrastructure for new Cloud

The Air Force currently has over 100 individually configured base enclaves that are not interoperable; each has its own access points to the outside world and internet. Control of these access points is critical to ensuring security as the Air Force begins to develop an organic core infrastructure for the new Air Force Cloud. The Air Force has taken the first step necessary to do this by establishing 16 gateways or “logical touch points” between the AFGIG and other, non-Air Force entities (both on NIPR and SIPR) as depicted in Figure 4 below.



Figure 4 New Gateway Configuration

The problem with this is it only addresses the network layer. Physical connections at each base still go through hundreds, if not thousands, of commercial circuits before linking back up at the 16 gateways. It is important that the core infrastructure of the new Cloud be built with all layers of the OSI model in mind. Simply limiting access at a logical layer does nothing to prevent access at the physical, transport, or application layer. Each layer hidden in a different packet, not readily accessible or viewable by all layers, only complicates the security process of current cyberspace platforms. The Air Force must be willing to look at the very devices and

techniques utilized to transmit data if it wants to change the operational environment to one that is controllable and defensive in nature.

If access to this new Air Force Cloud is to be limited, a holistic approach looking at the physical, application, network, and transport layer must be utilized. This could include, but not limited to, going to centralized security screening for untrusted traffic (firewalls, web proxies for inbound and outbound traffic), developing a new version of the internet protocol stack based on Air Force mission requirements, or utilizing NAT and proxy schemas to hide our assets in cyberspace. The good news with NAT is that it has way of causing incoming session connection requests not work because when a session request comes in from the outside, the NAT device doesn't know to which internal host this request should go.³⁰ This could be implemented today and would prevent many of the standard threats faced on the network without creating a problem for internal communications or outgoing session requests generated internally.

Changing from packet-based protocols to session-based protocols is also an option. As discussed earlier, using Session-Initiation-Protocol (SIP) which is designed to address the functions of signaling and session management within multimedia communications or a similar type protocol is a viable option. Signaling allows link information to be carried across network boundaries for positive identification of end-point users before access is granted. Session management provides the ability to control the attributes of an end-to-end call. Point-to-point session-based protocols could determine the location of target endpoints through address resolution, name mapping, and link direction. They would allow for identification of endpoint capabilities and security levels and restrict transmissions to only those classifications authorized for that endpoint user. These session-based protocols could be configured to eliminate multi-party connections when security requirements necessitated doing so, requiring the termination of

³⁰ Beijnum, Ljitsch, Everything You Need to Know About IPv6, Arstechnica, 7 March, 2007

both endpoints whenever one end was lost. Another aspect of limiting access to the Air Force Cloud is to ensure it is only used for official business.

Gone are the days when the Air Force can afford to let its employees surf the Web for sports, shopping, and the myriad of other actions personnel are performing on the web each day that are not mission related. Not every desktop or laptop in the Air Force requires access to non-military sites for their daily duties, with most sites needed being behind the portal. This goes back to step 1 of this process where the mindset with the Air Force must change. Internet access from Air Force systems is not a right, but more of a privilege that has restrictions on its application which has been abused or misused by many Air Force members. The rigor built into the core infrastructure identified above must also be carried over to the development of applications.

Step 4 - Build Application Security throughout Lifecycle

History has taught us that the Air Force focuses on a very small area of application security prior to deployment and even less after it is deployed. The Air Force must learn to expand its focus to include all phases of an applications lifecycle, from development through deployment and decommissioning. In the context of applications security, the Air Force should use the model shown in Figure 5 to ensure all known, necessary aspects of applications security are adapted for full coverage—no “gaps.”

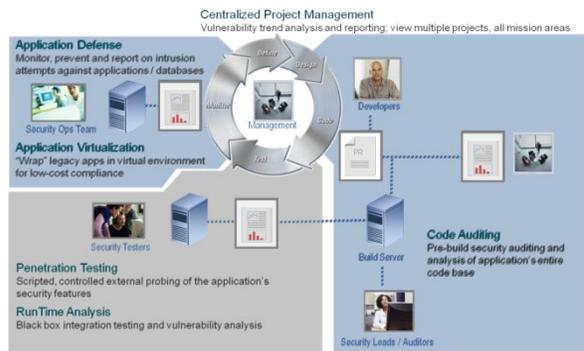


Figure 5 Building in Security during Entire Project

Applications need to have security baked in, not bolted on after development. Trying to make corrections to the entire code base after development is complete can be problematic and

cause software failures and vulnerabilities. The Air Force needs to take responsibility for the development of software programs that handle or process its most sensitive data and not rely on COTS or private companies for this. By building or developing its own applications, it will be easier to utilize emerging polymorphic technologies to defend them. This will also allow for an easier transition to effectively operate and defend the Cloud once established.

Step 5 - Build Operations Security

The Air Force has long known the advantage of maneuver on the battlefield, but has failed to translate that to the cyber environment. It has used static IP addresses for its most critical equipment for years, basically providing its adversaries with a fixed target upon which to focus. Technology is available to change this to polymorphic systems with agility and diversity built in which continually changes addresses, aka maneuverability. Often unreadable by the normal computer user with terms like “A fast and provably secure polymorphic block cipher consisting of a three-round Luby Rackoff pseudorandom permutation generator with a decorrelation stage employing a large number of interdependent pseudo-random number generators, combiner routines and permutation functions,” these technologies are gaining in popularity.³¹ Polymorphic techniques will allow unrestricted virtual maneuverability of data and assets in such a manner as to avoid threats by not staying in place long enough to become a target. Incorporated within polymorphic capability needs to reside a formally verifiable instance of commander’s intent, rules of engagement, courses of action, and Air Force policy that can react within nanoseconds of the onset of a cyber attack.³² The Air Force needs to embrace this new speed of warfare where a perceived view of reality may be only partially correct and trusts

³¹ Roellgen, C. B., *Turbo PMC V3 – 1024 bit block Cipher for Storage Device Block Level Encryption*, 6 November 2008.

³² Jabboore, Kamal, Dr., “IA + THE SCIENCE & TECHNOLOGY OF CYBER WARFARE”, PowerPoint briefing for Air War College IO Seminar, 4 Sep 2008

between man and machine is the inherent realm of the cyber warrior. A successful cyber strategy depends on the commander's ability to deliver timely effects and power assets to dominate the enemies decision cycle and exploit opportunities as they evolve in the unpredictable "Fog and Friction" of war.³³ Automated cyber capabilities allow the commander to establish priorities ahead of time, build in commander's intent into those capabilities, and operate with those capabilities at cyber speed. Only with these types of technologies can the Air Force hope to operate in a contested cyberspace environment to ensure it will be the key enabler it was designed to be.

Summary

Accepting cyberspace as a new warfighting domain implies the need to develop new doctrine and strategies to fly fight and win in that environment. US adversaries are much aware of Air Force increasing dependence on cyberspace and are looking for ways to exploit that dependence.³⁴ What the Air Force has done to date in cyberspace has had limited success in securing its networks and the current network attack-focused mindset must change. Our first challenge in cyber warfare will likely be to survive an initial attack, recover in a contested environment, and then defeat our adversary.³⁵ A meaningful strategic defense strategy is possible in cyberspace, without relying on the use of force for self-defense. The first priority in a defense-oriented network is to avoid the threat if at all possible, if not, then one must try to defeat the threat, and if that is not possible, then one needs to be able to survive the threat and continue to operate. The Air Force must create a trusted platform to conduct operations in cyberspace and instantaneously engage/defeat threats and attacks with systems and information

³³ Stein, George J., "Information War – Cyberwar – Netwar". Battlefield of the Future. Chapter 6, September 1995

³⁴ Fahrenkrug, David T. *The Age of Cyber Warfare*. The Wright Stuff November 29, 2007

³⁵ Ratazzi, Paul E., "CYBER DEFENSE CHALLENGES", PowerPoint briefing for Air War College IO Seminar, 4 Sep 2008

that can survive in a contested domain, as well as recover from damaged assets when necessary.

This all has to happen in a matter of nanoseconds, the speed of the 21st century.

Bibliography

- Air Force Cyber Command (Provisional), *Concept of Cyber Warfare*, 26 November 2007.
<http://www.afcyber.af.mil/>
- Air Force Cyberspace Command (Provisional) Programming Plan 09-01, *Air Force Cyberspace Command MAJCOM Activation*, 22 May 2008.
- Air Force Cyber Command. *Concept of Operations*, Draft version 4, 21 December 2006
- Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, 17 November 2003.
- Air Force Doctrine Document (AFDD) 2, *Operations and Organization*, 3 April 2007.
- Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 11 January 2005.
- Air Force Institute of Technology. *Center for Cyberspace Research*. <http://www.afit.edu/ccr/>
- Air Force Strategic Plan 2006-2008. <http://www.airforcestrategynet.mil/>
- ARPANET 1970s, Cyberte telecom Federal Internet Law and Policy,
http://www.cyberte telecom.org/notes/internet_history70s.htm
- Arwood, Sam. *Cyberspace as a Theater of Conflict: Federal Law, National Strategy and the Departments of Defense and Homeland Security*. Wright-Patterson Air Force Base, OH, Air Force Institute of Technology, Graduate School of Engineering and Management, June 2007.
- Beijnum, Lljitsch, Everything You Need to Know About IPv6, Arstechnica, 7 March, 2007,
<http://arstechnica.com/hardware/news/2007/03/IPv6.ars>
- Berkowitz, Bruce, "Information Warfare: Time to Prepare." *Issues in Science and Technology*, Winter, 2000. <http://www.nap.edu/issues/17.2/berkowitz.htm>
- Bickers, Charles, "Innovation, Cyberwar, Combat on The Web". *Far Eastern Economic Review*, August 16, 2001
- Bingling, Leng, Yulin, Wang, and Wenxiang, Zhao. "Bringing Internet Warfare into the Military System is of Equal Significance with Land, Sea, and Air Power." *Jieangjun Bao* (Chinese military newspaper), 11 November 1999, cited in *Intelligence*, N. 107, 29 November 1999.

- Brooks, Todd, Col, USAF, Zucco, Anthony, Col, USAF, Worley, Dean, Lt Col, USAF, and Davis, James, Lt Col, USAF. "Presentation of AFCYBER Forces: A Hybrid Approach." Professional Studies Paper. Maxwell AFB, AL: Air War College, 2008.
- Calle, Dan, CS 3604 Assignment, *Supercomputers*, Spring 1997, <http://ei.cs.vt.edu/~history/SUPERCOM.Calle.html>
- Cline, Brian, "Information Security Systems Engineering", *Cyber Crime Conference* PowerPoint briefing on 16 Jan 2008
- Convertino, Mike, Lt Col, USAF, DeMattei, Lou Anne, and Knierim, Tammy, Lt Col, USAF. "Flying And Fighting In Cyberspace." Maxwell AFB, AL: Air University Press, 2007.
- Courville, Shane P. *Air Force and the Cyberspace Mission: Defending the Air Force's Computer Networks in the Future*. Maxwell Air Force Base, AL, Center for Strategy and Technology, Air War College, 2007.
- Crampton, Jeremy W. *The Political Mapping of Cyberspace*. Chicago, University of Chicago Press, 2003.
- Cullather, Nick. "Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar." *Intelligence and National Security*, 18:4 <http://dx.doi.org/10.1080/02684520310001688907>
- Deptula, David A., Lt Gen, USAF. "Toward Restructuring National Security." *Strategic Studies Quarterly*, Vol. 1, No. 2 (Winter 2007)
- England, Gordon. "The Definition of "Cyberspace." Dep SECDEF Memorandum to Secretaries of Military Departments, et al., 12 May 2008. <http://www.afei.org/documents/NewCyberspaceDefinition.pdf>
- Fahrenkrug, David T. *The Age of Cyber Warfare*. The Wright Stuff November 29, 2007. <http://www.maxwell.af.mil/au/aunews/archive/0222/Articles/TheAgeofCyberWarfare.html>
- Fahrenkrug, David T. *Cyberspace Defined*. <http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html>
- Gates, Robert M., Secretary of Defense "SECDEF Memo C2 for Military Cyberspace Missions". Nov 08
- Gaudin, Sharon and Greenemeier, Larry. *Cyberwarfare: A Realistic Appraisal*. InformationWeek No. 1141:49 June 2007.
- Gaudin, Sharon, "Protecting a net in a time of terrorism", Network World, 09/24/01. http://www.nwfusion.com/archive/2001/125631_09-24-2001.html

- Gerhard, William E. Jr., Lt Col, USAF, Palmieri, Richard S., Lt Col, USAF, and Odom, Cecily A. "United States Air Force Presentation of Cyberforces to the Joint Force Commander." Professional Studies Paper. Maxwell AFB, AL: Air War College, 2008.
- Gerstein, Daniel M. *Leading at the Speed of Light: New Strategies for U.S. Security in the Information Age*. 1st ed. Washington, Potomac Books, 2006.
- Gerstein, Daniel M. *Securing America's Future: National Strategy in the Information Age*. Westport, CT, Praeger Security International, 2005.
- Gettle, Mitch, MSgt, USAF, Air Force Releases New Mission Statement, Air Force Link, 8 December 2005, <http://www.af.mil/news/story.asp?id=123013440>
- Goldsmith, Jack L. and Wu, Tim. *Who Controls the Internet?: Illusions of a Borderless World*. New York, Oxford University Press, 2006.
- Grant, Rebecca. "The Dogs of Web War." *Air Force Magazine*, Vol. 91, No. 1, January 2008. <http://www.afa.org/magazine/jan2008/0108dogs.html>
- Grant, Rebecca. *Victory in Cyberspace*. Arlington, VA, Air Force Association, 2007. <http://www.afa.org/media/reports/victorycyberspace.pdf>
- Greenemeier, Larry. *Cyberwarfare: By Whatever Name, It's on the Increase*. InformationWeek No. 1145:32 July 2-9, 2007.
- Grimes, John G., Assistant Secretary of Defense, Networks and Information Integration. *Department of Defense Net-Centric Spectrum Management Strategy*, Arlington, VA, August 3, 2006.
- Hall, Bill, Col, USAF."Force Development for Cyber Transformations". PowerPoint briefing for Air Staff, Oct 2008
- Hare, Forrest B. "Air Force Strategy for Cyberspace." *The Wright Stuff*, 29 November 2007.
- Harrington, Caitlin. "USAF Explores Development of Cyberspace Warfare Doctrine." *U.S. Air Force Aim Points*, 4 January 2008. <http://aimpoints.hq.af.mil/display.cfm?id=23233>
- Headquarters United States Air Force Program Action Directive (PAD) 07-08, Change 1, *Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER)*, 24 January 2008.
- Hildreth, Steven. *Cyberwarfare*. Library of Congress Congressional Research Service Report, 19 June 2001. <http://www.au.af.mil/au/awc/awcgate/crs/rl30735.pdf>

Hinote, Clint, Lt Col, USAF. "Air-Mindedness In Cyberspace: What Airmen Bring to the Emerging Domain." *The Wright Stuff*.
<http://www.maxwell.af.mil/au/aunews/archive/0303/Articles/AirMindednessinCyberspace.html>

Jabboure, Kamal, Dr., "IA + THE SCIENCE & TECHNOLOGY OF CYBER WARFARE", PowerPoint briefing for Air War College IO Seminar, 4 Sep 2008

James, Clement. *The Main Internet Threats for 2008*, 24 December 2007,
<http://www.vnunet.com/vnunet/news/2206237/main-internet-threats-2008>

Joint Publication (JP) 3-0, *Joint Operations*, 17 September 2006, Incorporating Change 1, 13 February 2008.

Joint Publication (JP) 3-13, *Information Operations*, 13 February 2006.

Kehler, Robert C., General, USAF. "Shaping the Joint Fight in Air, Space, and Cyberspace." *Joint Force Quarterly* 49 (2nd Quarter 2008)

Leipman, James M. Jr. "Cyberspace: The Third Domain." *The Wright Stuff*, 13 December 2007.

Lewis, James A., "Securing Cyberspace for the 44th Presidency". *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Center for Strategic and International Studies, Washington, DC, December 2008
http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, Cambridge University Press, 2007.

Nielsen, Suzanne C. and Welch, Donald. *Teaching Strategy and Security in Cyberspace: An Interdisciplinary Approach*. *International Studies Perspectives* 4:133-144 May 2003.

National Institute for Standards and Technology (NIST) Special Publication 800-30: Risk Management Guide for Information Technology Systems, July 2002

Paulson, Arjn, Col, USAF. "AF Space Command Provides AFCYBER with Key Support." *Air Force Print News Today*, 6 March 2008.

Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection*, 22 May 1998.

Ratazzi, Paul E., "CYBER DEFENSE CHALLENGES", PowerPoint briefing for Air War College IO Seminar, 4 Sep 2008

Roellgen, C. B., *Turbo PMC V3 – 1024 bit block Cipher for Storage Device Block Level Encryption*, 6 November 2008.

- Sawyer, Ralph D., "Sun TZU – Art of War". Westview Press Inc, Boulder Colorado, 1994
- Shachtman, Noah, "Air Force Wobbles on Plan for Cyber Dominance." *Wired - Danger Room*. 19 June 2008. <http://blog.wired.com/defense/2008/06/marlborough-mas.html>
- Stein, George J., "Information War – Cyberwar – Netwar". *Battlefield of the Future*. Chapter 6, September 1995. <http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html>
- The Air Force Roadmap for the Development of Cyberspace Professionals 2008-2018*, 15 April 2008.
- The National Strategy to Secure Cyberspace*, February 2003.
- United States. Department of Homeland Security. *National Infrastructure Protection Plan*. Washington, 2006. <http://purl.access.gpo.gov/GPO/LPS71533>
- United States. Department of Homeland Security. *Protecting America's Critical Infrastructure - Cyber Security*. http://www.us-cert.gov/press_room/050215cybersec.html
- Weik, Martin H., *The ENIAC Story*, Ordinance Ballistic Research Laboratories, Aberdeen Proving Ground, Maryland, 1961, <http://ftp.arl.mil/~mike/comphist/eniac-story.html>
- Weiss, Geoffrey, Maj, USAF. "Exposing the Information Domain Myth." *Air & Space Journal* - Spring 2008.
- Woolley, Pamela L. *Defining Cyberspace as a United States Air Force Mission*. Wright-Patterson Air ForceB, OH, Air Force Institute of Technology, School of Engineering and Management, June 2006.
- Wilson, Clay. Information Operations, Electronic Warfare, and Cyberwarfare: Capabilities and Related Policy Issues. Library of Congress, Congressional Research Service Report, 2007. <http://handle.dtic.mil/100.2/ADA466599>
- Wynne, Michael W. Secretary of the Air Force. "Flying and Fighting in Cyberspace". *Air and Space Power Journal 21*, Spring 2007

Appendix A

THE SECRETARY OF DEFENSE MEMORANDUM



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

NOV 12 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS
AND INFORMATION INTEGRATION
COMMANDER, U.S. STRATEGIC COMMAND
DIRECTOR, NATIONAL SECURITY AGENCY

SUBJECT: Command and Control for Military Cyberspace Missions

There is a pressing need to ensure a single command structure is empowered to plan, execute, and integrate the full range of military cyberspace missions. To this end, effective immediately, Commander, USSTRATCOM is directed to place Joint Task Force-Global Network Operations (JTF-GNO) under the operational control of Commander, Joint Functional Component Command-Network Warfare (JFCC-NW).

The officer serving as the Director, National Security Agency (DIRNSA) retains the duties and responsibilities previously assigned as Commander, JFCC-NW.

The officer serving as the Director, Defense Information Systems Agency (DISA) will continue to serve as Commander of JTF-GNO and will remain responsible for providing the JTF-GNO network and information assurance technical assistance as required.

A handwritten signature in black ink, appearing to read "Robert M. Gates".



OSD 77716-08

