Air Force Institute of Technology
AFIT Scholar

Theses and Dissertations   Student Graduate Works

3-2008

Cyber Flag: A Realistic Cyberspace Training Construct

Andrew P. Hansen

Follow this and additional works at: https://scholar.afit.edu/etd

Part of the Computer Sciences Commons

Recommended Citation

Hansen, Andrew P., "Cyber Flag: A Realistic Cyberspace Training Construct" (2008). *Theses and Dissertations*. 1759.
https://scholar.afit.edu/etd/1759

This Thesis is brought to you for free and open access by the Student Graduate Works at AFIT Scholar. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of AFIT Scholar. For more information, please contact richard.mansfield@afit.edu.

المنارة للاستشارات
www.manaraa.com

CYBER FLAG
A REALISTIC CYBERSPACE TRAINING CONSTRUCT

THESIS

Andrew P. Hansen, Major, USAF

AFIT/GCS/ENG/08-10

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

المنارة للاستشارات
www.manaraa.com

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

المنارة للاستشارات
www.manaraa.com

AFIT/GCS/ENG/08-10

CYBER FLAG
A REALISTIC CYBERSPACE TRAINING CONSTRUCT

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Computer Science

Andrew P. Hansen, BS, MS

Major, USAF

March 2008

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

المنارة للاستشارات

www.manaraa.com

AFIT/GCS/ENG/08-10

CYBER FLAG
A REALISTIC CYBERSPACE TRAINING CONSTRUCT

Andrew P. Hansen, BS, MS
Major, USAF

Approved:

//SIGNED// 22 Jan 08
Paul D. Williams, Ph.D. (Chairman) date

//SIGNED// 22 Jan 08
Mark A. Kanko, Ph.D. (Member) date

//SIGNED// 22 Jan 08
Robert F. Mills, Ph.D. (Member) date

//SIGNED// 22 Jan 08
Richard A. Raines, Ph.D. (Member) date

المنارة للاستشارات
www.manaraa.com

AFIT/GCS/ENG/08-10

Abstract

Now is the time for Cyber Flag – initiating and implementing an effective, comprehensive and coordinated training environment in the relatively new, but quickly developing cyberspace domain. As is well understood, the rapidly unfolding challenges of cyberspace are a fundamental warfare paradigm shift revolutionizing the path to victory in future wars. Moreover, while only time will tell the full affect of cyberspace on Worldwide, National, and military security and interests, the development of cyberspace, in its early stages, appears to have equivalent magnitude to the development of air capabilities during the 20th Century. A significant test for the Air Force (indeed any organization with a credible presence in cyberspace) will be providing a realistic training environment that fully meets this challenge. The Air Force grew out of technology and employment of that technology (in conjunction with people, processes and doctrine) within the air domain to influence the outcome of war. Innovation early in the airpower era helped solidify a new war-fighting domain that proved decisive in the Second World War, ultimately paving the way for the creation of the United States Air Force as lead service for organizing, training, and equipping an air-minded military capability. The early air pioneers of the 1920's could not have imagined what airpower would evolve into and the same is true with cyberspace pioneers today.

Why create another Flag-level exercise? Realistic training (that which is effective, comprehensive, and coordinated) is crucial to success in time of war. Red Flag

المنارة للاستشارات
www.manaraa.com

provides critical training within the air domain but now with the evolution of cyberspace, a comprehensive training environment is necessary to meet this growing and broadening threat. The Chinese People's Liberation Army (PLA) now focuses on achieving battlefield gains through the full spectrum of kinetic and non-kinetic capabilities with realistic training exercises at the center of these efforts.

Red Flag has and continues to be a great tactical training exercise; Cyber Flag would use the best practices of Red Flag (and other realistic training venues) to define a future training environment for the cyberspace domain. This research presents justification and an outline for the development of Cyber Flag as well as a formal Concept of Operations (CONOPS). The CONOPS provides a starting point for the basic requirements, with three alternative courses suggested for implementing Cyber Flag. As an integral element of Cyber Flag, the Virtualized Intranet Platform for Exercise Realism provides a framework for a low-cost network infrastructure necessary as a basis for a realistic training environment.

There is no better training than the hands-on realism associated with participation in an exercise such as Red Flag. Secretary Michael W. Wynne has a vision for dominant operations in cyberspace "comparable to the Air Force's global, strategic omnipresence in air and space." This bold vision requires a combination of joint coordination, skilled forces and a realistic training environment to bring these efforts together; Cyber Flag is the suggested vehicle for accomplishing this.

المنارة للاستشارات
www.manaraa.com

Acknowledgments

I would like to express my sincere appreciation to my research committee, Dr Mark Kanko, Dr Bob Bills, and Dr Rick Raines, as well as my faculty advisor, Major Paul Williams, for their guidance and support throughout the course of this thesis effort. I would also like to thank my sponsor, Capt Larry Fortson, from the Air Force Research Lab’s Human Effectiveness Division for both the support and latitude provided to me in this endeavor. The encouragement and guidance from Mr. Tom Harrison was invaluable in producing this document. Finally, the love and understanding of my family provided the foundation integral to my success.

Andrew P. Hansen

للاستشارات المنارة
www.manaraa.com

Table of Contents

Page

المنارة للاستشارات

www.manaraa.com

المنارة للاستشارات

www.manaraa.com

المنارة للاستشارات

www.manaraa.com

المنارة للاستشارات

www.manaraa.com

List of Figures

المنارة للاستشارات
www.manaraa.com

List of Tables

المنارة للاستشارات

www.manaraa.com

Acronyms

8AF	8th Air Force
ACC	Air Combat Command
ACMI	Air Combat Tracking System
ACSC	Air Command and Staff College
AEF	Air Expeditionary Force
AETC	Air Education Training Command
AFB	Air Force Base
AFCA	Air Force Communications Agency
AFCYBER	Air Force Cyber
AFDD	Air Force Doctrine Document
AFEO	Air Force Experimentation Office
AF-GIG	Air Force Global Information Grid
AFI	Air Force Instruction
AFIOC	Air Force IO Center
AFIT	Air Force Institute of Technology
AFIWC	Air Force Information Warfare Center
AFM	Air Force Manual
AFNETOPS	Air Force Network Operations Command
AFNOC	Air Force Network Operations Center
AFRL	Air Force Research Lab
AFTTP	Air Force Tactics Techniques and Procedures
AIA	Air Intelligence Agency
ALCOM	Alaska Command
AOC	Air Operations Center
AOR	Area of Responsibility
ARSTRAT	Strategic Forces Army
ATG	Adversary Tactics Group
AU	Air University
BDA	Battle Damage Assessment
BDU	Bomb Dummy Unit
BFT	Blue Force Tracking
C2ISR	Command Control Intelligence Surveillance and Reconnaissance
CAOC	Combined Air Operations Center
CSAR	Combat Search and Rescue
CERT	Computer Emergency Response Team

المنارة للاستشارات

www.manaraa.com

CINC	Commander-in-Chief
CJCS	Chief of the Joint Chiefs of Staff
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COMAFFOR	Commander, Air Force Forces
CONOPS	Concept of Operations
CSAF	Chief of Staff of the Air Force
CSAR	Combat Search And Rescue
CT	Continuation Training
DARPA	Defense Advanced Research Projects Agency
DCI	Defensive Counter Information
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOC	Designed Operational Capability
DoD	Department of Defense
DOE	Department of Energy
DPG	Defense Planning Guidance
DT	Dynamic Targeting
EA	Electronic Attack
EBO	Effects Based Operations
EM	Electromagnetic
EMS	Electromagnetic Spectrum
EP	Electronic Protect
ES	Electronic Support
EW	Electronic Warfare
FDL	Fighter Data Link
FSU	Former Soviet Union
GCC	Geographic Combatant Commander
GIG	Global Information Grid
GNO	Global Network Operations
GSI	Global Strike and Integration
HAF	Headquarters Air Force
HHQ	Higher Headquarters
HQ	Headquarters
HUMINT	Human Intelligence
IA	Information Assurance

للاستشارات المنارة
www.manaraa.com

IADS	Integrated Air Defense System
IAS	Information Aggressor Squadron
IDS	Intrusion Detection System
IFT	Initial Flight Training
IMINT	Imagery Intelligence
IN	Intelligence Need
INL	Idaho National Laboratory
INOSC	Integrated Network Operations and Security Center
IO	Information Operations
IOS	Information Operations Squadron
IP	Internet Protocol
ISR	Intelligence Surveillance and Reconnaissance
IT	Information Technology
ITO	Integrated Tasking Order
IW	Information Warfare / Irregular Warfare
JCS	Joint Chiefs of Staff
JEFX	Joint Expeditionary Force Experiment
JFC	Joint Force Commander
JFCC	Joint Functional Component Command
JFCC-GSI	JFCC for Global Strike and Integration
JFCC-IMD	JFCC for Integrated Missile Defense
JFCC-ISR	JFCC for Intelligence Surveillance and Reconnaissance
JFCC-NW	JFCC for Network Warfare
JFCC-Space	JFCC for Space Operations
JIOPH	Joint Information Operations Planning Handbook
JIOWC	Joint IO Warfare Command
JOA	Joint Operations Area
JP	Joint Publication
JTF	Joint Task Force
JTF-GNO	Joint Task Force for Global Network Operations
JRTC	Joint Readiness Training Center
KVM	Keyboard Video Mouse
LAN	Local Area Network
LARIAT	Lincoln Adaptable Real-time Information Assurance Testbed
LMR	Land Mobile Radio
MAJCOM	Major Commands
MCCDC	Marine Corps Combat Development Command
MDMP	Military Decision Making Process

المنارة للاستشارات
www.manaraa.com

MDVA	Mult-Discipline Vulnerability Assessment
MEB	Marine Expeditionary Brigade
MILDEC	Military Deception
MOS	Military Occupation Specialty
MCO	Major Combat Operations
NACTS	Nellis Air Combat Tracking System
NAF	Numbered Air Force
NATO	North Atlantic Treaty Organization
NAVSTRAT	Strategic Forces Navy
NCC	Network Control Center
NCSD	National Cyber Security Division
NCW	Net Centric Warfare
NetA	Network Attack
NetD	Network Defense
NETOPS	Network Operations
NIPRNet	Non-secure Internet Protocol Router Network
NMS-CO	National Military Strategy for Cyberspace Operations
NOG	Network Operations Group
NOSC	Network Operations and Security Center
NS	Network Support
NSA	National Security Agency
NTC	Nation Training Center
NTTR	Nevada Test and Training Range
NW	Network Warfare
NWG	Network Warfare Group
NWW	Network Warfare Wing
OPLANS	Operations Plans
OPSEC	Operations Security
OPSEC	Operations Security
OSD	Office of Secretary of Defense
PA	Public Affairs
PAFD	People’s Armed Forces Department
PLA	People’s Liberation Army (China)
PRC	People's Republic of China
PSYOP	Psychological Operations
QDR	Quadrennial Defense Review
SCADA	Supervisory Control and Data Acquisition
SECAF	Secretary of the Air Force

المنارة للاستشارات
www.manaraa.com

SECDEF	Secretary of Defense
SIMTEX	Simulator Training Exercise
SIPRNet	Secret Internet Protocol Router Network
SNL	Sandia National Laboratory
STRATAF	Strategic Command Air Forces
TAC	Tactical Air Command
TADIL	Tactical Data Information Links
TCP	Transmission Control Protocol
TRB	Tactics Review Boards
TST	Time Sensitive Targeting
TTP	Tactics Techniques and Procedures
UCP	Unified Command Plan
UK	United Kingdom
UNAAF	Unified Action Armed Forces
UNWT	Undergraduate Network Warfare Training
US	United States
USA	United States Army
USAF	United States Air Force
USAFWS	United States Air Force Weapons School
USAWC	United States Air Warfare Center
US-CERT	US Computer Emergency Response Team
USD	United States Dollar
USMC	United States Marine Corps
USN	United States Navy
USSTRATCOM	United States Strategic Command
VIPER	Virtualized Intranet Platform for Exercise Realism
WEPTAC	Weapons and Tactics Conference
WIC	Weapons Instructor Course
WMD	Weapons of Mass Destruction
WPAFB	Wright-Patterson Air Force Base

المنارة للاستشارات
www.manaraa.com

CYBER FLAG

A REALISTIC CYBERSPACE TRAINING CONSTRUCT

> *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.*
>
> - 2005 USAF Mission Statement

I. Introduction

> *To develop anything, the underlying thought and reason must govern and then the organization must be built up to meet it.*
>
> - Brigadier General William 'Billy' Mitchell

> *Red Flag exercises, well known as training components of air warfare, will also become a staple of cyber warfare.*
>
> - Secretary Michael W. Wynne [17]

The Red Flag exercise, held six times per year at Nellis and Eielson Air Force Bases, routinely pits a coordinated team of 80+ airplanes against numerous realistic air threats and a robust array of surface-to-air missile systems as participants deliver weapons and airdropped cargo on realistic targets and drop zones. Most participants would agree that Red Flag provides the ultimate peacetime test of joint and coalition air operations, but a fundamental paradigm shift is the only way to meet Secretary Wynne's vision of a significantly enhanced cyber warfare environment. This change is so monumental that full implementation would fundamentally detract from the critical objectives of Red Flag.

www.manaraa.com

> *Beware lest you lose the substance by grasping at the shadow.*
>
> - Aesop

Cyber warfare is a “shadow” of the Red Flag primary mission which is to “maximize the combat readiness and survivability of participants by providing a realistic training environment,” which they accomplish superbly. [77]

> *Success demands singleness of purpose.*
>
> - Vince Lombardi

Conflicts occur when an exercise cannot meet the competing key training objectives of multiple participating groups, such as pilots and information operators. This is not to say that the objectives of one group are less important or detrimental to the other. It simply means that the existing venue can no longer serve these diverse groups of warriors because of growing threats and the needs for training to meet these threats. In short, the time is right for Cyber Flag.

Background and History of Exercise Development

The Red Baron I and II Reports summarized the results of the Air Force’s critical analysis of the air war over Vietnam some of which was declassified in the late 1990s [62]. Both reports cited the lack of training realism as a significant factor in the 75 percent decrease in enemy vs. United States aircraft kill ratios between Korea (10:1) and Vietnam (2.5:1) [8, 62]. In response, Pentagon staffers with a vision to improve training realism first created the Red Flag exercise concept in 1975. The Commander of Tactical Air Command, General Robert Dixon, approved the concept, and the first Red Flag began

المنارة للاستشارات
www.manaraa.com

in November 1975 [15]. Over 30 years later, the constantly improving Red Flag exercise continues to train joint and coalition air forces to operate in a realistic air combat environment. Red Flag is also a key reason for the overwhelming conventional military success of the United States in recent conflicts [9:63].

Black Demon to Bulwark Defender

The Air Force Information Operations Center (AFIOC) at Lackland AFB created the Black Demon exercise in 2000 to test the defensive posture of our military computer networks [48]. For many, Black Demon was the equivalent to Red Flag played out on computer networks. Participants defended critical command and control nodes from persistent attacks launched by trained adversaries from the 57th and 177th Information Aggressor Squadrons, the 92nd Information Warfare Squadron, and the National Security Agency. In 2006, the exercise integrated forces from the Army, Navy, and Marine Corps and was renamed Bulwark Defender. The expanded exercise focuses on computer network defense and as such provides the best venue for joint integration of forces dedicated to this mission area. It does not, to any significant degree, however, address the other elements of Information Operations (IO), such as electronic warfare and psychological operations, nor does it provide a training environment that integrates cyberspace defensive threats and offensive opportunities with those of air-breathing or space-based assets. To capitalize on current cyberspace best practices requires building on the success of the Red Flag model within a dedicated environment tailored to this new warfighting domain. Cyber Flag is the suggested vehicle for this change.

المنارة للاستشارات
www.manaraa.com

To Cyber Flag

Low-altitude aircraft employment proved to be impractical in the Vietnam War leading to the development of medium and high altitude tactics. Key to these tactics was the suppression of enemy surface-to-air missile systems. A training conflict arose when missile systems were electronically jammed during Red Flag, however, because participant's ability to react to those threats became limited. For many aircrew members, the first time they faced actual indications of a surface-to-air missile system was at Red Flag. To preserve this critical training requirement, General Wilbur L. "Bill" Creech developed the Green Flag exercise in 1978 to emphasize the enabling capabilities of electronic warfare (EW) [15:46]. The Green Flag exercise was the most robust exercise of EW assets in the world.

The present day struggle to integrate the new domain of cyberspace offers similar challenges. The breadth and revolutionary nature of waging war in cyberspace extends beyond the goals and objectives of Red Flag and thus suggests the need for a parallel and complimentary approach. The goal of Cyber Flag would be to exercise offensive and defensive cyberspace capabilities, closely mirroring how the Chinese have trained since the late 90's in their transformation from a "mechanized PLA force to an informationalized force" [14:1].

The Need for a Dedicated Realistic Training Environment

"Exercises should be planned and conducted in a way that reflects real war." [9:65]

www.manaraa.com

As alluded to in AFDD 2-1 above, implementing realistic training environments for US and coalition force employment is paramount to future military success. Through the successful use of continuous improvement principles, Red Flag has evolved over the years, spawning other realistic training venues. The most notable offspring of Red Flag are, Blue Flag to prepare operational planning staffs, Virtual Flag to utilize simulation and virtualized combat environments, and Green Flag to provide integration with ground forces urgently in need of close air support [9:66]. These exercises, as well as Bulwark Defender, provide realistic training environments for aircrew and network operators without diluting or detracting from the critical objectives of Red Flag. Currently, a realistic training environment dedicated to cyberspace defensive threats and offensive capabilities does not exist.

The Time is Right for Cyber Flag

Is there a need for a dedicated Flag focused on the employment of capabilities within cyberspace?

> *"Airmen will be sent into battles against both known enemy and the unknown. Regardless, we will be better prepared to fly, fight and win for our Nation thanks to advanced composite force training. Use these opportunities to innovate and improve our tactics, technologies and training. If we can continue to make ourselves more lethal and effective, then we will continue to dominate Air, Space and Cyberspace for the Joint Team."* [18]

As General T. Michael Moseley conveys above, realistic training in the Air Force must encompasses every possible threat within all possible arenas. This vision echoes the findings of the Red Baron Reports, the genesis of Red Flag. The proficiency of Airman waging this cyberspace war must be equal to that of warriors in the land, sea, air and space domains. This proficiency comes from a "train the way we fight" mentality

المنارة للاستشارات
www.manaraa.com

dictated by the foundational doctrine of AFDD 2-1, *Air Warfare* [9:65]. This thesis looks at current limitations to realistic training in cyberspace to provide justification and a way ahead for Cyber Flag.

Red Flag, Bulwark Defender, and to a lesser degree Blue Flag, have key and critical objectives unlike those envisioned for Cyber Flag. Cyber Flag will need to support the objectives of existing exercises by providing key insight into possible threats and offensive opportunities. As a stand-alone exercise, however, Cyber Flag highlights very specific threats and capabilities that are of limited utility to other exercise staffs because of conflicts with pre-existing, well-established, and vital training needs. Development of Cyber Flag would preserve the effectiveness of established existing training while embracing and enhancing the new domain of cyberspace, integrating capabilities drawn from across the services and coalition partners into one coherent effort. Bulwark Defender is a key exercise of joint defensive capabilities within cyberspace. Cyber Flag will expand on that focus, enabling a training environment that integrates both offensive and defensive cyberspace effects into the mainstream operational and tactical planning effort. A Joint Force Commander for Cyber Flag would have the capacity to call on IO options or capabilities as readily as a bomb or other kinetic weapons.

Using qualitative analysis techniques, the Military Decision Making Process (MDMP), and case studies of current realistic training exercises, this thesis provides insight into the necessary changes needed to make Cyber Flag a reality.

المنارة للاستشارات
www.manaraa.com

Implementing Cyber Flag

This research provides an outline for the development of Cyber Flag and a formal Concept of Operations (CONOPS). The CONOPS provides a starting point for the basic requirements, with three alternative courses for implementing Cyber Flag. As an integral element of Cyber Flag, the Virtualized Intranet Platform for Exercise Realism provides a framework for a low-cost network infrastructure necessary as a basis for a realistic training environment.

Preview

This thesis outlines the Cyber Flag development effort by first analyzing where we are and then looking to where we need to go within both the Air Force and the Nation as a whole.

Where We Are

Chapter II defines the current threats and offensive opportunities for waging war in the cyberspace domain. Chapter III highlights the definition of cyberspace. Chapter IV provides a comprehensive review of the realistic training development to date, while Chapter V provides insight into conducting operational planning within cyberspace.

Where We Need To Go

Chapter VI explores the methodology used in developing recommendations for a realistic training construct. Chapter VII provides specific proposals for the integration of cyberspace capabilities into existing exercises supported by Cyber Flag. Chapter VIII defines a concept for a dedicated exercise environment that fully integrates cyberspace

المنارة للاستشارات
www.manaraa.com

capabilities, Cyber Flag. Chapter IX provides a proof-of-concept for integrating the Joint IO Range (JIOR) with Red Flag using a mobile network replication system called the Virtualized Intranet Platform for Exercise Realism (VIPER). Chapter X summarizes the results and conclusions of this research effort and looks to the future by defining areas for additional related research.

The Air Force Mission – Air, Space, and Cyberspace

Cyberspace, as the third "pillar" in the US Air Force's Mission Statement, justifies a dedicated "Flag" to fulfill the training required "to deliver sovereign options for the defense of the United States of America and its global interest." Cyber Flag provides this environment without diluting the critical time tested mission of the 414th and 353rd Combat Training Squadrons (Red Flag):

> *"Since combat is no place to train aircrews, Red Flag provides a peacetime 'battlefield' within which our combat air forces can train. Inside this battlefield, aircrews train to fight together, survive together and win together"* [77].

The time is right to provide an analogous battlefield for the new breed of cyber warriors in which they train in concert with those fighting from and in air and space.

المنارة للاستشارات
www.manaraa.com

II. The Threats

> *If you know the enemy and know yourself, you need not fear the results of a hundred battles.*
>
> – Sun Tzu

The current threats within cyberspace range from nation-states to organized crime with nearly equivalent capabilities in all categories based on the low entry cost into this warfighting domain. One major aspect of developing dedicated and focused realistic training for the future is to identify a baseline threat and then build the appropriate tactics, techniques, and procedures (TTPs) to mitigate such a threat. The objective of base lining is to establish a starting point for generating TTPs that deal with all credible threats. When analyzing the threats within cyberspace, it is important to look at the full spectrum, from individual actors to government and military forces.

Hackers

While the stereotype of a *hacker* is that of a young, mostly harmless, teenager on a joy ride through various systems, the term *hacker* applies to a broad range of techno-savvy individuals who thrive on matching wits with the professionals who design and manage the best networks in the world. On one end of this spectrum are the merely curious who want nothing more than to break into vulnerable systems for the challenge, like solving a puzzle. In the article, *Understanding the Hackers Mind* the authors present this type of thought and behavior as an inherent trait of a hacker along with a strong need for acceptance within the hacker community [73]. What is not necessarily inherent in the hacker’s mind is the penchant for criminal activity.

المنارة للاستشارات
www.manaraa.com

> *“The Jargon File contains a bunch of definitions of the term `hacker’, most having to do with technical adeptness and a delight in solving problems and overcoming limits. There is a community, a shared culture, of expert programmers and networking wizards that traces its history back through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments. The members of this culture originated the term `hacker’. Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you’re a hacker. The hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics or music -- actually, you can find it at the highest levels of any science or art. Software hackers recognise these kindred spirits elsewhere and may call them "hackers" too -- and some claim that the hacker nature is really independent of the particular medium the hacker works in. There is another group of people who loudly call themselves hackers, but aren’t. These are people (mainly adolescent males) who get a kick out of breaking into computers and phreaking the phone system. Real hackers call these people ‘crackers’ and want nothing to do with them. Real hackers mostly think crackers are lazy, irresponsible, and not very bright, and object that being able to break security doesn’t make you a hacker any more than being able to hotwire cars makes you an automotive engineer. Unfortunately, many journalists and writers have been fooled into using the word `hacker’ to describe crackers; this irritates real hackers no end.* ***The basic difference is this: hackers build things, crackers break them****.”* [74]

As the above quote explains, “crackers” engaged in overtly criminal activity (such as identity theft, denial of service attacks, or defacing websites). Criminal activity is increasing fueled by the “white market,” which “exists to buy and sell software flaws (back-door vulnerabilities with no available patch to fix them)” and creating “a virtual arms trade in potentially significant security threats” [72]. This underground economy supports the “black market” which barters, among other things, stolen identities as well as networks of compromised machines (Botnets) for use in denial of service attacks [72]. Criminals have spent up to $75,000 for the use of computer vulnerabilities that enabled large-scale theft of personal information [72].

المنارة للاستشارات
www.manaraa.com

After recently attending the first-ever Dayton, Ohio hacker convention, *HackCon*, this researcher realized just what a diverse and technically fanatical group hackers are. The goal of this convention was to bring together the efforts of hackers worldwide to "take the word 'hacker' back" [60]. As mentioned above, hackers have historically been associated with those conducting illegal activity such as breaking into government computer systems. HackCon aimed at drawing a clear distinction between the activities of hackers and crackers. Increasingly, the pool of computer capabilities within the hacker community provides a remarkable depth and breadth of experience in identifying critical enemy attack vectors in cyberspace. In addition, skills enabled by this expertise, provide a largely untapped level of experience in the capabilities the military must establish among cyber warriors. Cyber Flag would provide a realistic training environment to build on the basic skill set in order to hone the capabilities of the fighting force as a whole.

Terrorist Organizations

As is well known, terrorists have increasingly turned to cyberspace as a means of both communication and attack. Recruiting hackers from around the world has allowed organizations like Al Qaeda to prosper in cyberspace. A 2005 *Washington Post* article highlights that Al Qaeda was "the first guerrilla movement to move from physical space to cyberspace" [66]. Web-based training, communications, and logistical support increasingly enable terrorists to conduct successful attacks on forces within Iraq [66]. This virtual base of operations enabled by the anonymous nature of the Internet also facilitates the distribution of detailed attack plans including satellite imagery and Global

المنارة للاستشارات
www.manaraa.com

Positioning System (GPS) coordinates. The activities of Al Qaeda are not limited to Iraq. As an organization without a state sponsor, Al Qaeda must rely on passive sponsorship, enabled largely through the Internet. There are as many as 17,000 Al Qaeda websites used for propaganda, recruiting, and fund raising [71]. Although there is increased potential for laws prohibiting the spread of terrorist ideals, it is difficult to suppress these websites because they often simply change addresses once discovered [71].

By multiplying these capabilities in proportion to the size of a larger force, one begins to get an idea of how capable a nation-state actor can become if they choose to emphasize cyberspace capabilities.

Russia v. Estonia

> *"The 10 largest assaults blasted streams of 90 megabits of data a second at Estonia's networks, lasting up to 10 hours each. That is a data load equivalent to downloading the entire Windows XP operating system every six seconds for 10 hours."* [68]

The removal of the Bronze Soldier war memorial in Tallinn prompted a massive Russian cyber attack, as described above, on web servers associated with Estonian government, newspaper, banks, and businesses in May 2007 [61]. While the Russian government denied the attack, the scale and resources involved may indicate otherwise. The attacks used a distributed denial-of-service attack from thousands of machines to crush the routers and switches comprising Estonia's digital infrastructure [68]. A heavy use of global Botnets, purchased on the black market, helped boost the number of machines involved in the attack, many of which were unknowing foot soldiers [68].

The capabilities of nation-state actors in cyberspace are increasingly finding their way to center stage. The recent assault on Estonia highlights the strength of the Russians

المنارة للاستشارات
www.manaraa.com

within the cyberspace domain. The attacks prompted a rapid response from both NATO and the European Union and sparked bitter debate on the legal aspects of such attacks.

Chinese IO Strategy

China has emerged as one of the most capable forces in cyberspace for a number of reasons, including the establishment of over-arching IO strategy, presence of conventional military capability gaps, increased national defense spending, focus on IO education, and increases in IO operational readiness levels.

Chinese IO strategy in some ways closely mirrors US IO doctrine due in part to China's suspected analysis of Joint Pubs 3-13, 3-13.1, Army Field Manual 100-3 and Joint Vision 2010/2020 [23]. Chinese IO strategy has also likely evolved from careful study of such information-intensive US military operations including Desert Storm and Kosovo, as well as Operations Enduring Freedom and Iraqi Freedom. It is important to note that actual documented Chinese IO doctrine is largely unavailable and most Chinese IO strategic views come from publicly released literature. The Chinese senior military leaders seem to realize that all future fighting forces will be increasingly dependent on access to and exploitation of information in the domains of air, sea, land, space, and cyberspace. The Chinese view of IO within cyberspace is a phenomenon that is changing the nature of war from one focused on seizing territory or destroying forces, to one seeking to paralyze the adversary's information systems and to destroy his will to resist [26]. The IO strategy of China drastically diverges from that of the US in that they believe in the application of Maoist principles with the responsibilities for executing IO laying not only in the hands of the military but with the civilian populace as well, the

المنارة للاستشارات
www.manaraa.com

New People's War [25]. Furthermore, China views their IO capabilities as a pre-emptive weapon to establish information dominance, believing that superior tactics can make up for inferior technology [25]. Key strategy components include attacking enemy command and control systems, tactics to attack enemy commanders and headquarters at every level, information deception/concealment procedures, and imbedded information technology weapons to include computer viruses [24]. Other objectives include [25]:

1) Targeting enemy networks linking political, economic, and military installations of a society in general.
2) Developing, improving and utilizing China's information weapons in a concentrated way.
3) Emphasizing mobile war in the context of IO.
4) Conscientiously organizing sabotage operations to exhaust and wear down the enemy.
5) Organizing specialized IO troops equipped to carry out IO against the enemy's information infrastructure.

The Chinese categorize IO into narrow and broad applications. Narrow IO consists of destruction of enemy command and control, electronic warfare, military deception, operational secrecy, and psychological operations [28]. Broad IO consists of computer virus warfare, precision warfare and stealth warfare [28].

China's Conventional Military Capability Gaps

An enormous gap separates China's conventional military capabilities from its aspirations to be a dominant world power. Cyberspace seems to be the domain the

المنارة للاستشارات
www.manaraa.com

Chinese feel offers an opportunity to be on par with (and possibly leapfrog) other major global powers. Whatever China's concerns and intentions, its capacity to act upon them in conventional military ways, hostile to US interests, is severely limited, and will remain so for many years [29]. This gap, coupled with China's desire to become a major economic/political power in the world community, makes asymmetric forms of warfare increasingly more attractive. Information Operations is an asymmetric capability that will allow China to engage a far more superior military. China continues to seek unorthodox methods and capabilities that avoid or undercut an adversary's strengths while inflicting disproportionate damage on the enemy [23]. There exist strong feelings among many Chinese military analysts that cyberspace will be the critical factor in successful future military operations. Information Operations provide relatively low-cost asymmetric weapons, which enable a long-range power projection capability against US forces that was never before thought possible [25]. This capability can reach directly into the American homeland to attack vulnerable critical infrastructures to influence or manipulate domestic public perceptions. This alone will have effects far beyond the limited power projection capabilities of China's conventional military forces [23]. China aims to leapfrog generations of technologies and capture supremacy in the cyberspace domain [23].

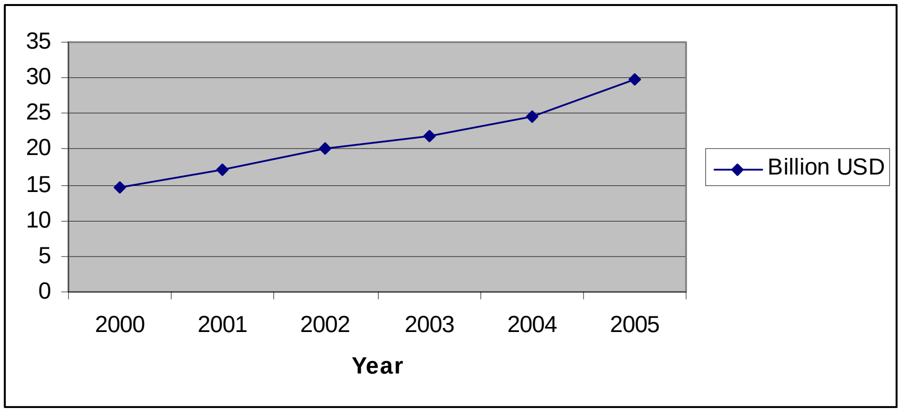
China's Increased National Defense Spending/Focus on IO Education

Other important factors in establishing China as a baseline cyberspace threat is their steadily increasing national defense budget and continued focus on IO education programs and institutions. As Table 1 shows, in 2000 the Chinese defense budget

المنارة للاستشارات
www.manaraa.com

exceeded 14.6 billion USD, an increase of 17.7 percent from the previous year, with the 2005 military spending at 29.9 billion USD.

Table 1 Chinese Defense Spending



The US government analysis anticipates double-digit percentage increases in Chinese defense spending over the next decade [31]. More importantly, China's defense budget may be as much as 40 to 70 percent higher than publicly released government budget estimates and at the current rate of growth, China will be spending more on defense than the US or any of its allies by the year 2025 [30]. This budget buildup stems from the urgent need to replace antiquated military equipment, establish and solidify a quality oriented manufacturing base and to bring about reform in weapons system acquisition. Information technology (IT) is one of the key areas that will receive a defense-spending windfall as a result [30]. China's IT sector is probably the most organizationally innovative and economically dynamic producer of equipment for China's military. China continues to invest in commercially applicable IT and broadly funds civilian and commercial research institutes which can conduct basic and applied IT research more effectively and efficiently than the military. China is also allocating major

للاستشارات المنارة
www.manaraa.com

resources to further IO education efforts, providing the Chinese military with indigenous IO capabilities and a professional cadre needed to wage the battles of tomorrow. There are several organizations charged with provided IO education to the Chinese military [14]:

1) The Communications Command Academy is the lead IO educational organization-providing curriculum in strategic analysis, operational/tactical requirements, command, and tactics.
2) The Information Engineering Institute aims to educate professionals in hi-tech warfare involving such areas as remote image information engineering, satellite navigation, position engineering, map data banks, information security, modern communications technology and space technology.
3) The Science and Engineering University provides initial IO education to new military personnel.
4) The National Defense Science and Technology University focuses on supercomputer technology, reconnaissance, monitoring technology, precision guidance technology, electronic warfare and information warfare.
5) The Navy Engineering College seeks to merge arms and information by integrating electronic information with weapons systems.

Moreover, the Chinese categorize the IO education and training audience into three categories [27]:

1) Senior leaders with little current information literacy
2) Future leaders that must enhance their information abilities

المنارة للاستشارات
www.manaraa.com

3) Younger personnel who are information savvy

Each category receives training in [27]:

1) Basic IO theory
2) Electronic warfare and radar
3) IO rules and regulations
4) IO strategy and tactics
5) Theater and strategic IO
6) Information systems
7) Command and control systems
8) Information weapons and applications
9) Simulated IO scenarios

From this perspective, it is apparent that the Chinese have established a sound educational base with both broad and focused training programs, potentially exceeding that of their United States counterpart.

China’s Increase in IO Operational Readiness Levels

The third major element in assessing China as the baseline cyberspace threat is their recent increase in IO operational readiness and simulated IO exercises. Because the Chinese believe that IO is the New People’s War, China’s strategy for executing IO operations falls largely on its 1.5 million-person reserve force. Currently, China is turning entire reserve force districts into mini IO regiments. The active military is still responsible for developing IO strategies and plans but civilians, more precisely the reserve forces, will be leading IO execution in battle. For example, the People’s Armed

المنارة للاستشارات
www.manaraa.com

Forces Department (PAFD) of the Echeng District has 20 city departments of militia/reserve IO regiments. These regiments consist of network warfare, electronic warfare, intelligence, and psychological warfare battalions as well as 35 technical squads. The PAFD also established the first reserve IO training base to serve these units. The city of Ezhou conducts national defense mobilization exercises, recruiting technical soldiers and procuring IT equipment for the National Defense Mobilization effort. The Fujan Province uses reserve and militia forces to carry out EW, network attack/defense, and radar reconnaissance operations. In the city of Datong, high-technology units focus on information security and seizing computer network domains [14]. China's intentions are obvious and there is increasing evidence that they are putting their IO theory and training into practice in state of the art realistic training environments. As indicated previously, there have been frequent reports of hacker attacks against the US that originate from China, an effort dubbed "Titan Rain" by the US Government [42]. The *Washington Post* reported in August 2000 that hackers connected to the Chinese government penetrated the Los Alamos computer system and downloaded sensitive information equivalent to a 3-foot high stack of paper [75]. A Los Alamos representative reported that enormous amounts of Chinese hacking activity hits Los Alamos continuously [75].

> *"During one 10-month period in the late 1990s, officials said, intelligence agencies recorded 792 computer security incidents, including 324 attacks from outside the United States. The attacks included efforts to gain password files, probes of computer defenses and scans of system vulnerabilities to intrusion. Several computer systems have been compromised by intruders who gained "root" access to Energy Department computer systems. Such access allows hackers to gain complete access and total control over computer systems that permit them to see all information on the systems, the officials said. Many of the*

المنارة للاستشارات

www.manaraa.com

> *attacks are from foreign intelligence services seeking restricted nuclear information or other sensitive material, particularly on science and technology."* [75]

A more recent attack on Los Alamos resulted in the compromise of visitor logs, including date of birth and social security numbers of thousands of scientists visiting the laboratory between 1990 and 2004 [76].

> *"The attack was described as being conducted through several waves of phishing emails with malicious attachments, starting on Oct. 29. Although not stated, these would presumably have launched Trojans if opened, designed to bypass security systems from within, which raises the likelihood that the attacks were targeted specifically at the lab."* [76]

China understands the importance of conducting IO exercises and does so quite frequently. These exercises test technologies, refining operational planning/procedures, tactics development, and network reconnaissance. The Chinese often target Taiwan and the US for their exercise scenarios. Recent IO exercises included the Chengdu Military Region conducting a confrontational Internet campaign exercise. This exercise provided training for the planning of an IO campaign with the overall goal of establishing information control of the adversary [27]. The Beijing Military Region conducted computer network campaigns aimed at reconnaissance, counter-reconnaissance, interference, counter-interference, blocking, air strikes, and counter-air strikes. The Chinese also conducted national exercises, as far back as 1998, aimed at uniting and coordinating several military regions throughout the country to test IO capabilities and assess their own weaknesses [14]. The Chinese are becoming increasingly more aggressive in their overall pursuit of IO techniques for counter-attack and cyber-defense.

www.manaraa.com

Cyber Flag would be a parallel US realistic training environment to prepare for and overcome this threat when called upon.

للاستشارات المنارة

www.manaraa.com

III. Cyberspace

There is something more important than any ultimate weapon. That is the ultimate position — the position of total control over Earth that lies somewhere out in space. That is . . . the distant future, though not so distant as we may have thought. Whoever gains that ultimate position gains control, total control, over the Earth, for the purposes of tyranny or for the service of freedom.

- Senator Lyndon B. Johnson, 1958

Before outlining the evolution of realistic training in cyberspace, it is important to refine the definition of this domain and the challenges associated with the Air Force becoming the lead service in cyberspace. The extraordinary challenges faced in integrating the decisive domain of cyberspace into the USAF mission are not unlike those faced in the infancy of the Air Force.

The Air Force grew out of technology and employment of that technology (in conjunction with people, processes, and doctrine) within the air domain to act as a deterrent to potential enemies and, when attacked, to successfully influence the outcome of war. Innovation early in the airpower era helped solidify a new war-fighting domain that proved decisive in the Second World War, ultimately paving the way for the creation of the United States Air Force as lead service for organizing, training, and equipping an air-minded military capability. Likewise, we are now in the infant stages of the cyber era where the addition of cyberspace is revolutionizing the way we will fight and win future wars. A significant challenge will be providing a realistic training environment that reflects this change. This is far different from the normal evolution of Red Flag over its 30-year history but is similar to the technological advancement comprising a core element in the history and mind-set of the Air Force. The early air pioneers of the 1920's

المنارة للاستشارات
www.manaraa.com

could not have imagined how airpower would evolve and the same is true with cyberspace today. In a recent *Letter to Airmen*, Secretary Wynne highlighted the incredible technological advancements, which are yet again transforming the face of war.

> *"Our adversaries realize the asymmetric opportunities of cyberspace. They attempt to access American industrial servers that contain sensitive data, exploit electromagnetic energy to try and jam or misdirect our precision weapons, and use radio transmitters to detonate improvised explosive devices, killing Americans, Coalition allies, and innocent civilians."* [3]

While the recent emphasis on cyberspace defense is a step in the right direction, US military preparations are equivalent at best to some other international powers, as noted earlier. Hardly a week goes by without some news report about how Chinese entities (government, military, or individual actors) have compromised computers and various US networks. This series of coordinated attacks beginning in 2003 (Titan Rain), is just one indication that the United States has already fallen victim to Chinese offensive information warfare activity [42]. One need also look at the recent public release of the Aurora experiment to understand the effects that are possible within cyberspace [43]. Although many of the details remain classified, Aurora demonstrated how one of the most commonly used power generators within the domestic electrical grid of the United States could be destroyed using computer network attack. During this test, the generator responds to a series of malicious computer control commands by shaking violently and then grinds to a complete halt in a cloud of smoke. The exploitation of this same vulnerability across the nation would bring extended power outages and crippling economic repercussions. Government economist Scott Borg summarizes the consequence of such an attack as follows:

المنارة للاستشارات
www.manaraa.com

> *"It's equivalent to 40 to 50 large hurricanes striking all at once," Borg said. "It's greater economic damage than any modern economy ever suffered. ... It's greater than the Great Depression. It's greater than the damage we did with strategic bombing on Germany in World War II."* [43]

Cyberspace Defined

The September 2006 cyberspace definition endorsed by the Joint Chiefs of Staff is:

> *"A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures."* [5]

Nearly two years later, there continues to be no published service or joint doctrine that defines cyberspace. This leads to differing views about what cyberspace comprises and what constitutes a force operating in this domain. Discussions within and across the services are complicated by a lack of common lexicon which clearly delineates what forces and capabilities (such as electronic warfare) fall within the cyberspace domain. Doctrine is fundamental to discussing, understanding, and coordinating warfighting in all domains. Doctrine also supports senior decision makers when dealing with the financial strain of the "long war." [44]

The services do have mature doctrine on information operations (IO), however. Air Force Doctrine Document 2-5, Army Field Manual 3-13, Marine Corps Warfighting Publication 3-36 and Joint Publication 3-13 comprehensively cover IO but the conceptualization of cyberspace as a domain is absent from nearly all formal military documents. Table 2 summarizes the terminology in current literature and formal doctrine used to define the domain in which the services conduct IO.

المنارة للاستشارات

www.manaraa.com

Table 2 Cyberspace Terminology in Doctrine

Service	Current Literature Terminology	IO Doctrine Terminology
Air Force	*Cyberspace* (8th AF CONOPS)	*Information Spectrum* or *Information Architecture* (AFDD 2-5)
Army	*Information Domain*	*Information Domain* (FM 3-13)
Navy	*Information Infrastructure*	*Information Infrastructure* (OPNAV 3430.26)
Marines	*Information Environment*	*Information Environment* (MCWP 3-36)
Joint	*Cyberspace (JCS)*	*Information Environment* (JP 3-13)

The inconsistency in cyberspace doctrine restricts our ability to integrate non-kinetic information operations and kinetic effects within the new domain of cyberspace. For example, if the Joint Force Commander requires a cyberspace effect, such as disrupting or destroying a command and control network, are we restricted to current IO capabilities? Most would agree that the answer is no.

What is a cyberspace effect? Dropping a bomb on a facility housing a critical network node could have an equal effect to that of injecting a computer virus that disables the network. Both options affect the adversary's ability to exchange data via their network and thus manifest themselves within the cyberspace domain. The explosive power of a bomb also has second and third order effects that ripple through the air and land domains making the computer virus attack potentially more appealing primarily due to the ease of reconstitution. In addition, a virus or other type of malicious software on an adversary machine may provide capabilities to the attackers even more valuable than the destruction of the network. Most people can conceptualize this because of the constant threat of Spyware infecting their personal computer. Few are aware of programs

المنارة للاستشارات
www.manaraa.com

called Rootkits that can cloak these activities within the inner workings of the computer operating system, making them undetectable by most, if not all, antivirus software. Debates regarding the use of non-kinetic versus kinetic options are just recently coming into mainstream military thought. China is far beyond these discussions, having already established consistent policy and doctrine, some of which is available through open sources, and an accompanying large-scale information warfare force that trains within realistic cyberspace environments [14].

In spite of how many credible experts have described it to date, the important reality of the cyberspace domain is that it encompasses far more than just computer networks. Cyberspace is a sphere that includes every element of both analog and digital data just as airspace includes every air molecule [5]. Cyber Warfare includes Network Warfare, Electronic Warfare, and Directed Energy as means of achieving effects within cyberspace. One need only look at the control these digital elements have over banking, power distribution, and personal communications to realize the true extent of this domain, a domain the military must defend. As Secretary Wynne recently wrote:

> *"Cyberspace is a domain, like land, where each of the principles of war applies. To grasp this concept requires a major institutional and cultural shift in war planning and operations."* [17]

The Chinese realized this some time ago and, in many respects, capitalized on the fact that the United States has not emphasized the enabling capabilities of operations within and through cyberspace. The conduct and resulting effects of information operations may not be as visually impressive as kinetic operations involving physical destruction, but an effective IO offensive capability, on a large-scale basis, provides

المنارة للاستشارات
www.manaraa.com

destructive potential on par with wide scale employment of nuclear weapons. In fact, due to our own dependence on cyberspace, the US is more susceptible to asymmetric attacks against our cyberspace infrastructure than we are to conventional attacks. The rapidly advancing technology (typically developed far quicker than appropriate defensive countermeasures) that makes our country so powerful represents a giant Achilles heel for which we must develop the most effective and cost efficient techniques to protect it before the first large-scale paralyzing 9/11 cyberspace event.

Cyberspace Fighting Force

With this vulnerability in mind, the proper posturing of forces to wage war in cyberspace is critical to the future of the Air Force and our nation. Thus, 18 September 2007 brought the activation of the Cyber Command (provisional) at Barksdale AFB under Major General William T. Lord [45]. An accompanying force development effort for this new major command will bring personnel from various career fields (such as electronic warfare, communications, and space control) which are critical to cyberspace operations. The Cyber Command compliments both the Naval Network Warfare Command and the Army 1st Information Operations Command with respect to joint operations. The Air Force now fully embraces cyberspace as an operational domain; a domain in which we attack and defend targets, achieve effects, and hold adversary capabilities at risk. In keeping with this theme, Cyber Flag provides the training compliment to and for Cyber Command.

A recent Air & Space Power Journal article *Defining Information Operations Forces* [37] comprehensively covered the capability gaps within and between the services

المنارة للاستشارات

www.manaraa.com

regarding the IO mission. This work contends that these gaps exist primarily since previous attempts to define and build a dedicated IO force were unsuccessful [37]. Cyber Command establishes the leadership to build a robust force but, as discussed earlier, pitfalls still exist because of the slow evolution of military doctrine for cyberspace. Although doctrine must eventually catch up to capabilities in cyberspace, an effective training environment provides a viable springboard for avoiding the current hazards.

Joint and service doctrine, such as Air Force Doctrine Document 2-1, *Air Warfare*, clearly and consistently defines missions conducted within the air domain, such as Offensive Counter Air and Close Air Support. The IO doctrine on the other hand, has morphed several times in the last decade as we struggled to define IO in a language that best supports the war-fighting mission. This has led to variation between the service level doctrine and confusion when integrating joint IO capabilities. Current joint doctrine is the final authority for these service level inconsistencies. The IO core capabilities, as defined by Joint Publication 3-13, encompass Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC), Electronic Warfare (EW), and Computer Network Operations (CNO). Table 3 summarizes their definitions.

These core capabilities define operations within an “information environment,” which consists of physical, information, and cognitive domains [7]. As suggested earlier, we have an approved DoD definition of cyberspace, but it is not immediately clear how cyberspace meshes with this information environment. Further, we have yet to decipher cross-domain operations, for example, operations through cyberspace that may yield physical effects (like Aurora), and vice versa.

المنارة للاستشارات
www.manaraa.com

Table 3 Joint IO Capabilities [7]

IO Capability	JP 3-13 (13 Feb 06) Definition
PSYOP	*Planned operations to convey selected truthful information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of their governments, organizations, groups, and individuals.*
MILDEC	*Those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly forces' mission.*
OPSEC	*A process of identifying critical information and subsequently analyzing friendly actions and other activities to: identify what friendly information is necessary for the adversary to have sufficiently accurate knowledge of friendly forces and intentions; deny adversary decision makers critical information about friendly forces and intentions; and cause adversary decision makers to misjudge the relevance of known critical friendly information because other information about friendly forces and intentions remain secure.*
EW	*Any military action involving the use of electromagnetic (EM) and directed energy to control the EM spectrum or to attack the adversary.*
CNO	*Capabilities used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure.*

We will continue to struggle with effective inter-service integration without a commonly accepted understanding of what cyberspace is (and is not). Fortunately, we are seeing more publication of ideas, such as the recent A&SPJ article *Cyberspace Defined* [38]. *Cyberspace Defined* clearly articulates the fact that cyberspace is a domain and delineates the fact that Information Operations are one of several means of achieving effects within this new domain. The Air Force has struggled with communicating this fact since the addition of cyberspace to the mission.

www.manaraa.com

Further adding to the confusion, and frequently impeding progress, is the current convention in military circles to attach the word “cyber” to any concept remotely associated with the cyberspace domain. This leads to terms like “cyber doctrine”, “cyber forces” or simply “cyber capabilities.” Such terminology tends to blur the overall concept of cyberspace as warfighting domain on par with air, land, sea and space operations. As an example, consider that information operations (things we do to achieve effects) should not simply be lumped into cyberspace (an environment in which we do things). Performing information operations in not limited to just cyberspace. Many psychological and military deception operations are not limited to the cyberspace domain but rather are classic instances of IO. One example would be the common practice of distributing leaflets like the one in Figure 1 which says “Osama bin Laden $25,000,000 reward [47].”

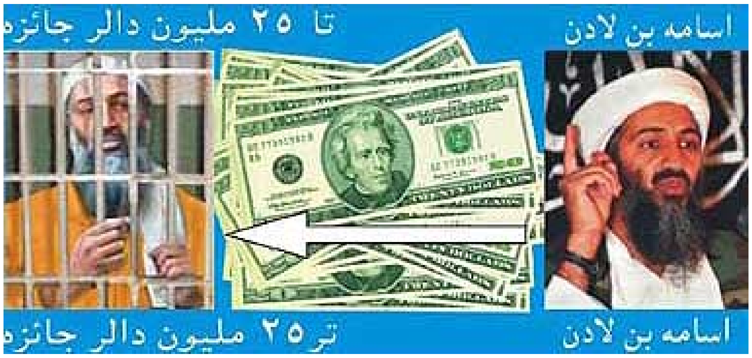


Figure 1 IO PSYOPS Outside of Cyberspace [47]

Doctrine typically defines how forces are organized and employed within a domain rather than describing the domain itself; in which case, the term “cyber doctrine” is inappropriate. “Cyber capabilities” describes capabilities solely within and through

المنارة للاستشارات
www.manaraa.com

cyberspace but perhaps it is more appropriate to use IO to describe these capabilities for the sake of consistency. As discussed above, there are kinetic capabilities that manifest themselves in cyberspace. Should we consider these "cyber capabilities?" Is the pilot who drops the bomb on a network building and ultimately disables the information flow a "cyber operator?" Such questions are not new, but the result is that cyberspace defines a domain in which we conduct operations; doctrine is how we formally define and discuss those operations. Force structures across the services must consistently conform to this model.

Definitions are vital for providing a common understanding among the diverse organizations that conduct operations within cyberspace. Another important issue regarding the cyberspace definition is that it encompasses far more than just computer networks. As noted earlier, Secretary Wynne describes cyberspace is a domain that includes every element of both analog and digital media just as airspace includes every air molecule [5]. With this idea in mind, it is easy to realize the broad range of skills that war fighters within this domain require. Current training in fundamental network operations builds the basic skill set [37]. Expertise on foreign and domestic cyberspace systems must also extend from outside Internet Protocol (IP) based networks and to applications that are more pervasive; such as telephony, Supervisory Control and Data Acquisition (SCADA) and Command and Control systems. The nexus of a comprehensive knowledge base on the vulnerabilities of all network systems comes from the legal and technical expertise gleaned through realistic training envisioned in and by Cyber Flag. Because of the stealth and speed of hacker attacks (the Slammer Worm

المنارة للاستشارات

www.manaraa.com

propagated worldwide in minutes), those capabilities defending our systems must be able to react incredibly quickly to prevent follow on attacks [6]. This is a defensive problem that the government must address, while adjusting to offensively fight and win in the new domain of cyberspace. The existing literature highlights a strong set of cyber capabilities but a poor ability to communicate these to Joint combatant commanders [39]. Cyber Flag is a practical application of these capabilities that will require the commonality within the services in order to achieve success facing a credible cyberspace threat. To fly and fight in Cyber Flag will require consistent doctrine, consistent joint definitions, and refined roles for warriors conducting operations in the cyberspace domain.

While the Air Force begins organizing, training, and equipping a force for cyberspace operations, we face the fact that much of the expertise rests with civilians. However, this was equally true of the pioneering air domain as well, because most of the early air pioneers were civilian enthusiasts. The ability to leverage the capability of computer hackers who are so often trying to penetrate government and civilian networks offers incredible potential in the initial realistic training environment (if nothing more than using these experts as training combatants). Consider that during the early years of aviation some of the most respected pilots were those seen performing unimaginable aerial demonstrations as stunt pilots and barnstormers. Regarded as renegades, these same pilots pushed aircraft capabilities and performance to their limits and as a result, names like Charles Lindbergh, are indelible in the history of aviation. In many respects, hackers test our information systems in many of the same ways and are an invaluable resource as the Air Force and Defense Department seek the skills required to gain

المنارة للاستشارات

www.manaraa.com

dominance in the cyberspace domain. The capability to defend against the best computer hackers in the world will enable the military to leapfrog the civilian sector cyberspace capabilities in much the same way that the USAF now certainly dominates the air domain. The overall goal is to develop a future *shock and awe* expertise providing strong deterrent to potential enemies and the assurance, if foolishly attacked, that decisive battlefield actions would minimize damage to US military and civilian personnel as well as their assets. The most effective way to integrate this cutting edge expertise is by creating an environment that highlights, demonstrates, and improves the enabling capabilities of cyberspace. This environment is Cyber Flag.

المنارة للاستشارات
www.manaraa.com

IV. Realistic Training Evolution

> *The battle of Waterloo was won on the playing fields of Eton.*
>
> - Lord Wellington

> *Desert Storm was won at the Nellis ranges and the US Army's National Training Center.*
>
> - AFDD 2-1

> *I'd hate to see an epitaph on a fighter pilot's tombstone that says, "I told you I needed training." . . . How do you train for the most dangerous game in the world by being as safe as possible? When you don't let a guy train because it's dangerous, you're saying, "Go fight those lions with your bare hands in that arena, because we can't teach you to learn how to use a spear. If we do, you might cut your finger while you're learning." And that's just about the same as murder.*
>
> - Colonel 'Boots' Boothby (First 64th Aggressor Squadron Commander)

Cyber Flag is representative of the fields of Eton and the Nellis ranges for the looming cyberspace threat the United States, and indeed the civilized world, will inevitably face. Realistic training exercises exist at the strategic, operational, and tactical levels of war. Broadly speaking, these levels of war utilize the Diplomatic, Informational, Military, and Economic (DIME) instruments of power and exercises provide the necessary realism to prepare forces across this spectrum.

The strategic level of war focuses on employing national power less by military and more through the D, I, E elements of DIME. Strategic warfare is most commonly associated with the deterrent capabilities of nuclear weapons but increasingly cyberspace weapons are becoming the tools of choice [63: 2]. The operational level of warfare

المنارة للاستشارات
www.manaraa.com

focuses on fighting and winning a campaign (the M in DIME), while the tactical level consists of the force-on-force battles supporting the operational effort. As an example, at the strategic level, the United States used diplomatic appeal through the United Nations, economic sanctions, and a robust media campaign (IO) to persuade Iraq to withdraw from Kuwait prior to the Gulf War in 1991. When these efforts failed, the operational campaign, Desert Storm, used military might to force Iraq out of the region. A series of tactical battles waged from the air, land, and sea supported the overall goal of this Desert Storm campaign.

Training is an integral part of coordinating these strategic, operational, and tactical efforts during wartime. War games are the training vehicle for strategic warfare [9:65]. Operational exercises focus on conducting campaigns through the assignment of missions, tasks and resources to tactical operations. Tactical exercises focus on the tactics, techniques, and procedures (TTPs) developed to employ weapon systems against an adversary.

The following sections describe current realistic training in more detail while Table 4 summarizes the prominent exercises in which the Air Force participates. Appendix A provides a more comprehensive primer for military training exercises not covered in this chapter.

Strategic Exercises

The most prominent wargaming venues in the Air Force are Unified Engagement (UE) and Future Games (FG), also known as the Future Capabilities Game. These exercises, held every two years, validate the future acquisition efforts of Joint and

www.manaraa.com

Coalition forces by using strategic moves and a credible military force structure to fight a conference room battle. Both the red and blue teams brief their plan at the end of each day and the assessment cell evaluates the successes and failures associated with each move. Future Games 07, held at the Air Force Wargaming Institute at Maxwell AFB, AL on 14-19 Oct 07, was the first exercise to highlight the increasing role of Information Operations at the strategic level of war. This game utilized forces operating in cyberspace to achieve strategic, operational, and tactical objectives. This validated the conclusions of a 1998 RAND study highlighting the increasing asymmetric effects of Information Warfare at the strategic level of war [63].

Operational Exercises

The Blue Flag and Terminal Fury exercises are prime examples of operational exercises. The Tactical Air Command developed the Blue Flag exercise in 1977 to provide realistic training to Combined Air Operations Center (CAOC) staff members [50]. The CAOC is a complex and unique weapons system and as such requires great proficiency from those who operate it. The Blue Flag CAOC controls mostly simulated assets with the information systems seldom attacked, prompting organizers to incorporate more live fly participants and an increasing number of network intrusions by trained information aggressors. Terminal Fury is a US Pacific Command exercise, which began in October of 2002 to test the contingency response of the Joint Task Force 519 [55]. This is an operational-level planning exercise similar to Blue Flag but encompassing joint and coalition partners.

المنارة للاستشارات
www.manaraa.com

Table 4 Prominent Training Exercises

Exercise	Location	Focus	Level	Off/Def	Agency
Unified Engagement	PACAF HQ	Future acquisitions (10 years)	Strategic	Off	HAF/A5XS
Future Games	AFWI	Future acquisitions (20 years)	Strategic	Off	HAF/A8X
Red Flag	Nellis AFB and Eielson AFB	Large force fam. (first 10 missions)	Tactical	Off	414 CTS and 353 CTS
Green Flag (East and West)	Nellis AFB and Barksdale AFB	CAS integration with Army	Tactical	Off	549 CTS and 548 CTS
Blue Flag	Hurlburt AFB	CAOC Staff	Operational	Def	505 CTS
Virtual Flag	Kirtland AFB	C2	Operational	Off	705 CTS DMOC
Black Demon	Barksdale AFB	AF C2 processes	Tactical	Def	23 IOS
Bulwark Defender	Barksdale AFB	Joint C2 processes	Tactical	Def	STRATCOM
JEFX	Nellis AFB	Research and devel.	Operational and Tactical	Off	AWFC
Terminal Fury	Hawaii and Japan	Joint Task Force training and integration	Operational	Off	JTF 519
Mission Employment	Nellis AFB	Large Force planning and empl.	Tactical	Off	USAFWS
Maple Flag	Cold Lake, CA	Large force fam.	Tactical	Off	CAF 4th Wing
Northern Edge	Alaska	Homeland Defense	Operational/ Tactical	Off/Def	Alaska Command

المنارة للاستشارات
www.manaraa.com

These exercises provide unparalleled training for operational planners. Blue Flag, however, has logically avoided large-scale integration with offensive and defensive cyberspace operations due to the potential conflicts with existing core training; in particular, the generation of the Air Tasking Order (ATO). A computer network attack that prevents generation of an ATO would result in a conflict with the critical training associated with the objectives of Blue Flag.

Tactical Exercises

The focus of tactical exercises is the force-on-force application of military power with Red Flag being the most prominent example. The CSAF approved the Red Flag Concept of Operations (CONOPS) on 15 July 1975 and the first exercise began on 27 November 1975 [15]. For over 30 years, aircrew members have faced the tactical challenges of Red Flag played out on the 1,000 square-mile Nevada Test and Training Range (NTTR). Crews plan and execute day and night missions often employing live munitions against realistic targets while facing aggressor aircraft and simulated surface-to-air missiles. The success of Red Flag resulted in the creation of similar tactical exercises to provide realistic training in other critical areas. Cope Thunder, Maple Flag, and Air Warrior provided realistic training for integrated strike packages conducting both interdiction and Close Air Support (CAS) missions. These realistic training venues created an incredible leap in pilot proficiency and lethality. As is reflected in AFDD 2-1, “Desert Storm was won at the Nellis ranges and the US Army’s National Training Center” [9].

المنارة للاستشارات
www.manaraa.com

Red Flag has also given rise to realistic tactical training in computer network defense. In 2000, the 23rd Information Operations Squadron (IOS) conducted the first Black Demon exercise [52]. This exercise brought a Red Flag flavor to the Computer Network Defense (CND) environment. Black Demon used both live and simulated networks to focus on the defense of the entire Air Force network hierarchy [52]. The simulated network provided the capability for more realistic attacks while the live play enabled testing and training of the communication capabilities from the lowest level Network Control Center (NCC), through the Network Operations Security Center (NOSC) for each major command, up to the Air Force Network Operations Security Center (AFNOSC). This exercise quickly gained credibility and gave rise to a joint exercise called Bulwark Defender in 2006.

The Air Force coordinated the Bulwark Defender exercise in 2006 under the guidance of US Strategic Command (STRATCOM), Defense Intelligence Agency (DIA), National Security Agency (NSA) and the Joint Staff [53]. The exercise challenges network operations supporting the Army, Navy, Air Force and Marines under one Joint umbrella. This exercise has become the annual Joint Information Assurance (IA) / CND capstone event, allowing collaboration within the DoD and civilian sector on the best methods for protecting the Global Information Grid (GIG) [53]. Regarding the success of this event, Col Gary McAlum, Director of Operations for Joint Task Force- Global Network Operations stated:

> *"This was an excellent opportunity to exercise strategic-level NetOps tactics, techniques and procedures with a tactical context. Bulwark Defender emphasized the necessity for near-real-time collaboration in dealing with incidents at base*

www.manaraa.com

> *level that can quickly have implications across the global information grid. Old stove-pipe reporting processes just don't cut it in this battlespace."* [53]

This quotation highlights the reality that cyberspace effects encompass all levels of war, strategic, operational, and tactical. Although Bulwark Defender is a tactical exercise, it allows participants to realize the global effects enabled through cyberspace. Network operators see and understand these effects. The difficulty is now illuminating the rest of the Air Force and Department of Defense as to these challenges and opportunities.

Combined Exercises

Increasingly, the Red Flag and Northern Edge exercises combine the operational and tactical aspects of warfare. In these exercises, the ATO generated by the CAOC dictates the tactical objectives of each day's missions thus bridging the operational and tactical boundaries. As a result, these exercises provide the most realistic representation of how Joint and Coalition forces fight wars. Those participating in these exercises find how complex modern warfare is and how dependent we are on information. The information supporting Red Flag and Northern Edge is trusted implicitly for a number of reasons, most notably safety. The reality is, however, that it is unlikely this level of trust in information will exist in real war.

The Black Demon and Bulwark Defender exercises focus on the hands-on tactical defense of networks supporting the CAOC and the operational planning effort as a whole. Computer networks are constantly under attack and network operators attempt to mitigate this onslaught. A significant limitation, however, is that the information flowing on these

المنارة للاستشارات
www.manaraa.com

networks does not currently translate to offensive tactical employment in air, space, or cyberspace, however. In other words, the ATO and associated planning products produced by the CAOC during these exercises do not put weapons on targets. The reason for this is understandable; the Bulwark Defender and Black Demon exercises train warriors to defend critical information networks and accomplish this task very well. This does highlight the fact, however, that there is no current venue combining operational planning with putting weapons on target in a hostile cyberspace environment. These weapons are not just bombs and, as discussed previously, offensive cyberspace capabilities employed at the tactical level can have strategic effects on par with our nuclear arsenal.

Evolution of IO training

The exercises described above all have specific objectives but none of them provides the capability to demonstrate the dominant and comprehensive effects capable through cyberspace envisioned in and by Cyber Flag.

المنارة للاستشارات

www.manaraa.com

V. Information Operations Planning

> *IO capabilities can produce effects and achieve objectives at all levels of war and across the range of military operations.*
>
> \- JP 3-13

As described in the previous chapters, the addition of *cyberspace* to the USAF Mission Statement marks the recognition of a new dimension in war fighting [1]. This comes on the heels of two other revolutionary concepts: Net Centric Warfare (NCW) and Effects Based Operations (EBO). One reality of the current transformation of war fighting is the movement from an attrition-based to an effects-based mindset with cyberspace as a key medium. The NCW construct is central to this metamorphosis in that everything from our battlefield weapon systems to each individual decision maker comprise a network node with linkages enabled through cyberspace. The scale of these networks varies widely depending on whether we are executing a contingency-level operation, Irregular Warfare (IW), or a Major Combat Operation (MCO) against a nation-state-level adversary [2]. A second reality is that cyberspace is itself a domain that enables the realization of significant combat effects; a truth clearly understood by those engaging in asymmetric terrorist operations. The cyberspace domain is the haven for terrorists using the electromagnetic spectrum (primarily the Internet and cell phones) as an enabling medium to launch asymmetric attacks against the United States and its allies. For this reason, IW has become the near-term focus of military efforts as the 2006 Quadrennial Defense Review highlights [4]. Cyberspace affects all activities within IW and MCO. Fundamental to the transformation from attrition-based to effects-based

المنارة للاستشارات
www.manaraa.com

employment is the change in the way we train. An environment encompassing kinetic and non-kinetic effects allows EBO to become the model for fighting wars. This transformation must also include scenarios incorporating the near-term realities of Irregular Warfare with the future inevitability of Major Combat Operations.

The Cyberspace Battlefield

If the warfighting domain consists of coordinated systems (net-centric), then outcomes depend on either severing the links between those systems (network nodes) or affecting the nodes themselves. Achieving control in all mediums linking these nodes (air, space, and cyberspace) encompasses a broad range of tasks (effectors) that support EBO. As an example, dropping a bomb on a network node achieves similar results through the air medium that a denial of service attack on that same node accomplishes through cyberspace. The Cyberspace Primer at Appendix B provides additional insight into characterizing these linkages by using models.

One of the most effective cyberspace effects (which is largely absent from kinetic employment) is the impact of interference resulting in a distrust of critical systems and information. Currently, information is generally trusted (by US forces), almost implicitly, but achieving distrust is relatively simple using any numbers of Computer Network Attack (CNA) methods. Consider the following example, which highlights the significant operational impact resulting from an underlying distrust of the data feeding a network.

The Combined Air Operations Center, which produces the ATO for Red Flag, uses an intranet to link the many computers coordinating the operational planning effort.

المنارة للاستشارات
www.manaraa.com

This network contains several ties to the outside world in order to enable access to the Internet and Global Information Grid. Using a relatively low level of sophistication, with no long-term damage, an adversary could penetrate the network and cause various computers to display the adversary nation’s flag as the desktop background and screen saver. In itself, this action is benign but requires access to the computer file system that, if achieved, would also allow theft or modification of data that users would not likely ever know about. The result can and should be a loss of confidence in the data and information on the affected machines and the network as a whole. The reaction of the commander would likely range from a simple incident response and forensic analysis to momentary termination of planning activities. Although the primary effect is to delay ATO production, there would be a strong possibility of rippling effects in the targeting cycle. This is just one of multiple possible scenarios that require training to ensure adequate preparation during an actual crisis.

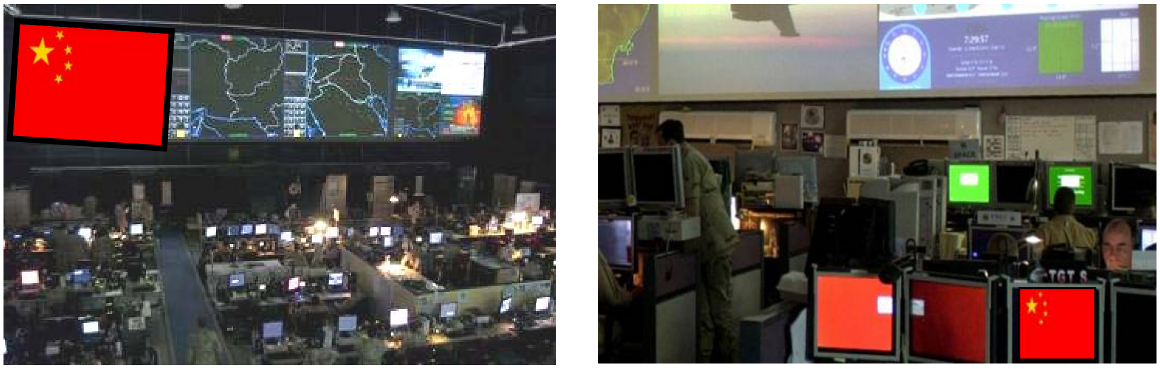


Figure 2 Trust Compromise

www.manaraa.com

Training Gaps

Currently, a training gap exists in showing exercise participants how the analysis of effects and consequences within all domains link directly to the military objectives. For example, to conserve weapons during training, aircrews often drop BDU-33s (25-pound inert training munitions) on the designated target while simulating a much larger conventional combat load. By comparison, we can demonstrate compromise in the trust of a system or network by simply modifying the background display of an AOC as described above. This would effectively simulate a broader virus insertion that could destroy the data on each machine encountered.

Another gap in the training environment is the lack of network diversity. As discussed previously, IP networks form the foundation of our nation's information infrastructure. It is, therefore, critical that expertise in IP networks remain the core knowledge base for those responsible for defending US civilian and military systems. However, the cyber battlefield is not limited to IP-based networks. In fact, the current definition of cyberspace extends beyond networks encompassing the broader areas of electronic warfare (EW) and Space Control, as well as Command and Control systems and Network Warfare [7].

Achieving Cyberspace Superiority

Recent conventional operations, such as Desert Storm, Iraqi Freedom and Allied Force, depended on air superiority. By definition, air-superiority *"enables friendly forces to use the air medium for military purposes while denying the enemy effective use of the same"* [9:2]. A very clear and critical future objective must be superiority that *"enables*

www.manaraa.com

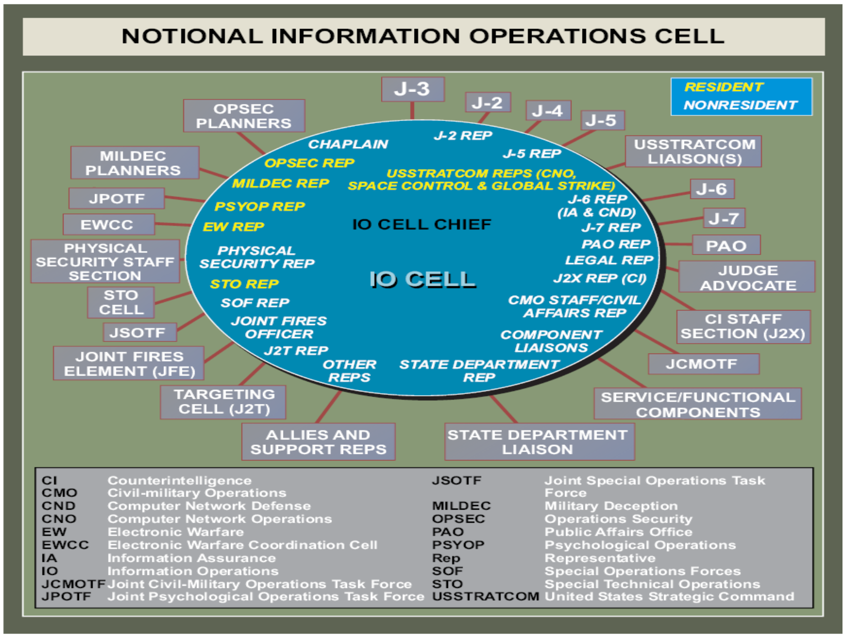
friendly forces to use the <u>digital</u> medium for military purposes while denying the enemy effective use of the same" [9:2]. Just as General "Hap" Arnold saw the key role that the airplane would play in the next major conflict, so must leaders today see the role of the computer or other devices capable of achieving effects in cyberspace (inhibiting or modifying data and information).

Defining Target Sets in Cyberspace

A target set is the subset of available targets, which, if destroyed, achieve the desired effect. An initial question we must address and answer is how do we define target sets in cyberspace? This is a very crucial element of fighting the war within this new domain, yet there is very little existing guidance on the topic. The joint doctrine guidelines dictate that an IO Cell (Figure 3) or planning organization be a component of the overall war planning effort in evaluating battlefield targets [7]. A similar understanding exists within the Air Operations Center (AOC) for planning Air Force missions. In addition, "*the Joint Force Commander should tailor the composition of the cell as necessary to accomplish the mission"* [7].

The J-2T component of the cell represents the targeting team residing under the J-2 (Intelligence) arm of the Joint Operations Center [7]. This targeting team is responsible for developing target sets that meet the Joint Force Commander's intent in accordance with the Joint Targeting Cycle (Figure 4). The Joint Prioritized Integrated Target List prioritizes these targets and the planning cell then assigns them to a specific day's mission via the Integrated Tasking Order (ITO) [32].

المنارة للاستشارات
www.manaraa.com



CI	Counterintelligence	JSOTF	Joint Special Operations Task Force
CMO	Civil-military Operations		
CND	Computer Network Defense	MILDEC	Military Deception
CNO	Computer Network Operations	OPSEC	Operations Security
EW	Electronic Warfare	PAO	Public Affairs Office
EWCC	Electronic Warfare Coordination Cell	PSYOP	Psychological Operations
IA	Information Assurance	Rep	Representative
IO	Information Operations	SOF	Special Operations Forces
JCMOTF	Joint Civil-Military Operations Task Force	STO	Special Technical Operations
JPOTF	Joint Psychological Operations Task Force	USSTRATCOM	United States Strategic Command

Figure 3 Information Operations Cell [7]

The ITO designates specific details as to the means of destruction for each of the targets (platform and weapon).

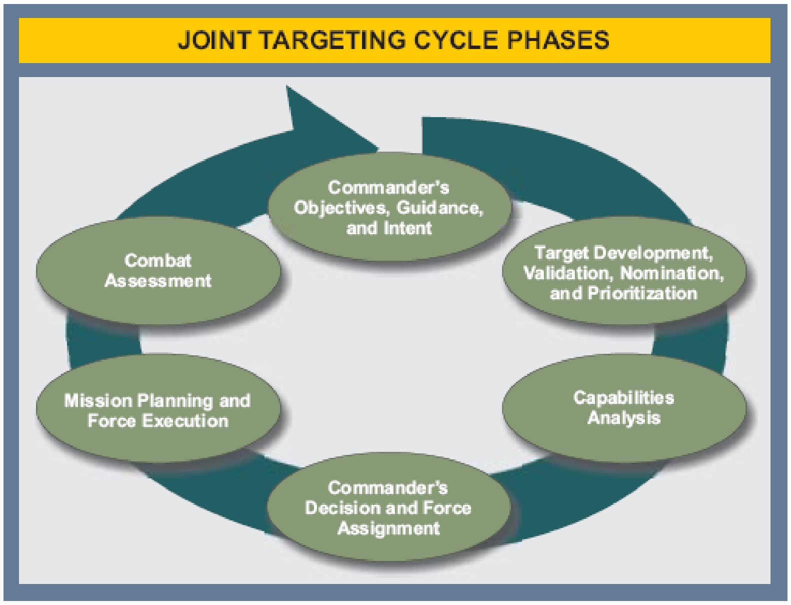

JOINT TARGETING CYCLE PHASES
Commander's Objectives, Guidance, and Intent
Target Development, Validation, Nomination, and Prioritization
Capabilities Analysis
Commander's Decision and Force Assignment
Mission Planning and Force Execution
Combat Assessment

Figure 4 Joint Targeting Cycle [32]

المنارة للاستشارات
www.manaraa.com

This is a very complicated process, involving a multitude of factors, and there is very little guidance to aid the planner within the Air Force or Joint Community. The Joint Staff drafted the *Joint Information Operations Planning Handbook (JIOPH)* in 2003 to provide the necessary guidance to the J-2T on how to target IO threats [33]. While this document does provide greater fidelity, it fails to provide adequate guidance for target selection. *Joint Tactics, Techniques and Procedures for Intelligence Support to Targeting* (Joint Pub 2-01.1) also attempts to provide clearer guidance for IO planning but succumbs to the same shortfalls as JIOPH [32]. Narrowing the field, by separating the most critical component of the IO battlefield (Computer Network Operations), is an essential starting point in defining an effective planning process. Cyber Flag enables this capability by allowing the targeting of critical routers and communications nodes with the resulting effects directly tied to the exercise objectives.

Cyberspace Weaponry

An effective Cyberspace strategy must also include a credible and effective method of selecting the appropriate weapon to neutralize or destroy a cyberspace target. These weapons and tactics can range from conventional kinetic weapons to the unconventional virus infiltration of an enemy’s command and control network. The USAF Intelligence Targeting Guide defines the term “weaponeering” as “the process used to effect the desired destruction on a specific target” [34]. The following are critical elements of the weaponeering process for conventional weapons directly applied to cyberspace targets [34]:

المنارة للاستشارات

www.manaraa.com

1) Establish the damage criteria (e.g., permanent destruction versus temporary incapacitation)
2) Determine available weapons and their effectiveness
3) Determine aim points and desired impact points
4) Evaluate weapon effectiveness post attack

These targeting guidelines do not currently exist in the IO arena and this is likely the reason why warfighting commanders seldom turn to the IO Cell to eliminate targets. The importance of IO (not cyberspace) is found in all current joint doctrine but specifics on how to employ this capability are largely absent throughout.

An effective offensive cyberspace strategy requires weaponeering criteria. Once accomplished, intelligence-gathering activities on network configurations and vulnerabilities will predict weapon effectiveness and enable probabilistic battle damage assessment. Mapping and studying enemy network configurations, just as we do physical structures, identifies key vulnerabilities. Once known, we can then predict the effect of a particular cyber weapon. This defines the planning process for conventional attacks and there is a direct correlation to cyber targeting. The destruction of computer network architectures with a cyber weapon is analogous to penetrating and destroying multi-story hardened bunkers with laser-guided munitions. As such, we must extrapolate tools like the Joint Munitions Effects Manual, to cyber weapon employment [34]. This would allow mapping of Integrated Tasking Order targets to cyber weapons providing the critical link required in the kill chain. The IO Cell can communicate cyber weapon capabilities by using much more familiar conventional weapon comparisons.

المنارة للاستشارات
www.manaraa.com

Assessment

After the completion of an attack, battle damage assessment (BDA) analyzes planned effects compared to the actual outcomes. The criteria outlined in the J-2 targeting guidance describe the following critical areas in evaluating IO weapon effectiveness [34]:

1) Corruption
2) Deception
3) Delay
4) Denial
5) Disruption
6) Degradation
7) Destruction

These areas are currently more challenging to evaluate in the CNO arena because, some say, a deterministic process may not be possible or practical, but in any case, the expertise in this area has not been developed [34]. For example, how do we really know we have disabled a targeted computer if we do not have physical access to it? As such, there must be a probabilistic model to convey the results of a network attack. The necessity to use a predictive process in evaluating attack success has given rise to the development of Effects Based Operations (EBO) which provide a means to "anticipate direct and indirect effects of a specific action" [35]. This concept uses modeling to predict the outcome of a specific attack and will undoubtedly play a necessary and

المنارة للاستشارات
www.manaraa.com

integral part in convincing commanders that cyber weapons are a viable (and often the best) choice in destroying critical targets.

Brig Gen William “Billy” Mitchell faced numerous obstacles when attempting to convince military leaders that aviation would define the outcome of future wars; many of the same struggles exist today in the cyberspace arena. There is a decisive need for a refined plan to weaponeer information technologies. With China representing the baseline threat, the United States must establish a concrete cyberspace employment plan including target sets, “weaponeering,” and employment standards all rigorously tested through Cyber Flag.

المنارة للاستشارات
www.manaraa.com

VI. Research Methodology

> *In the development of air power, one has to look ahead and not backward and figure out what is going to happen, not too much what has happened.*
>
> - Brigadier General William 'Billy' Mitchell

This chapter describes the research methodology, data collection and analysis for the development of an effective, efficient, and realistic cyberspace-training paradigm. This research centers on the case study design methods outlined by Robert Yin [69]. Yin defines six sources of evidence in support of case studies [69:30]:

- Documentation
- Archival Records
- Interviews (primary source for this research due to the scarcity of literature)
- Direct Observations
- Participant-Observations
- Physical

Using these evidence sources and the *Theory-Building* methodology of Yin [69:54], the first six chapters outline a historical analysis of realistic training exercises and the evolution of employment within the cyberspace domain. Chapter VII outlines the integration of the cyberspace elements into existing training venues based on this same analysis.

In addition to historical analysis, this researcher conducted a series of data collection interviews between August 2006 and August 2007 (Table 5).

المنارة للاستشارات

www.manaraa.com

Table 5 Visited Organizations

ORGANIZATION	LOCATION	POC
AFRL/HE	Mesa, AZ	Dr Dee Andrews
AFRL/HEX	Wright-Patterson AFB, OH	Capt Larry Fortson
HAF/A8X	Pentagon	Group Captain Gibson
AWFC/CC	Nellis AFB, NV	MajGen R. Michael Warden
57 ATG	Nellis AFB, NV	Col David Stilwell
57 IAS	Nellis AFB, NV	LtCol Reb Butler
57 IAS	Nellis AFB, NV	LtCol Robin Williams
57 IAS	Nellis AFB, NV	Capt Kristin Steinke
57 IAS	Nellis AFB, NV	Capt Josh Benson
57 IAS	Nellis AFB, NV	Capt Chris Evans
64 AGRS	Nellis AFB, NV	LtCol Greg Marzolf
65 AGRS	Nellis AFB, NV	LtCol Larry Bruce
18 AGRS	Eielson AFB, AK	LtCol Patrick Welch
343 OG	Eielson AFB, AK	Col Mark Moore
AFIOC, Det 2	Nellis AFB, NV	Mr Jim Hird
AFRL/HEAS	Mesa, AZ	Dr Joe Weeks
NASIC/ADEA	Wright-Patterson AFB, OH	Mr Kieth Bobick
NASIC/ADCC	Wright-Patterson AFB, OH	Mr Karl Harvey
NASIC/ACDI	Wright-Patterson AFB, OH	Mr Craig Johnson
33 IAS	Lackland AFB, TX	LtCol Mike Harasimowicz
AWC/CSAT	Maxwell AFB, AL	LtCol Steve Moscarelli
8AF/A3	Barksdale AFB, LA	LtCol Dave Fahrenkrug
8AF/A3	Barksdale AFB, LA	Major Tim Franz
8AF/CV	Barksdale AFB, LA	MajGen John W. Maluda
67 NWW	Lackland AFB, TX	Mr John Dougherty
ASC/XRA	Wright-Patterson AFB, OH	Mr Tim Menke
ASC/XRA	Wright-Patterson AFB, OH	Mr John Silance
AFRL/SNZW	Wright-Patterson AFB, OH	Mr Mike Foster
Booz Allen Hamilton	Lackland AFB, TX	Dr Mark Kanko
67 OSS	Lackland AFB, TX	LtCol Paul Harrington
USSTRATCOM/JFCC-GSI	Tinker AFB, OK	Major Chris Fogle
353 CTS	Eielson AFB, AK	LtCol Brett Pauer
HAF	Washington, DC	MajGen Charles V. Ickes II
AFRL/RI	Rome, NY	Dr Kamal Jabbour
MIT Lincoln Laboratory	Boston, MA	Dr Rob Cunningham
MIT Lincoln Laboratory	Boston, MA	Mr Lee Rossey

المنارة للاستشارات
www.manaraa.com

These interviews targeted agencies that are integrating IO into training and test environments. Most dialogues involved the presentation of research methodology as well as a formal interview. Due to the immaturity of cyberspace as a fully developed Air Force mission area, the interviews proved to be the most valuable source of data.

Trip Reports

June-August 2007; Air Force Research Lab, National Air and Space Intelligence Center, Aeronautical Systems Center, Wright-Patterson AFB, OH: The data collection process started at Wright-Patterson AFB with visits to several agencies conducting research and development of technologies supporting warfare within cyberspace. Captain Larry Fortson is leading the efforts of the Air Force Research Lab's Human Effectiveness Division in developing concepts and technologies that will ultimately improve capabilities in cyberspace.

Mr. Mike Foster is the director of the Virtual Combat Lab (VCL) within the Sensors Directorate of AFRL. The VCL provides an incredible capability to test electronic warfare and network attack tools against realistic threats. The VCL develops and improves capabilities used by Mr Tim Menke at the Aeronautical Systems Center to validate procurement decisions for the Air Force. The VCL also supports threat exploitation efforts conducted by Mr Keith Bobick and Mr Karl Harvey at the National Air and Space Intelligence Center.

June-October 2007; Future Games 2007, Chantilly, VA and Maxwell AFB, AL: Participation in the Future Games 2007 exercise proved the most fruitful series of trips because of the topic evaluated and, more importantly, the people involved. Through

المنارة للاستشارات

www.manaraa.com

three planning conferences and the game itself, this researcher was able to talk with some of the key participants in the development of Cyber Command, including LtCol Fahrenkrug (8th Air Force) and LtCol Harasimowicz (33rd IAS). These individuals provided key insight into the integration efforts of LtGen Elder and the 8th Air Force staff as well as key issues in the standup of Cyber Command. In addition, FG 07 enabled an audience with MajGen Warden (AWFC/CC) and Col Stilwell (ATG/CC). This was critical, in that, these individuals are responsible for the advancement of existing realistic training in the form of Red Flag, Virtual Flag, Green Flag, and Blue Flag.

June 2007; Air Force Research Lab, Rome, NY: A Cyber Defense Conference provided the perfect opportunity for this researcher to brief the focus of this thesis and to interact with individuals such as Dr Kamal Jabbour who have tremendous insight into the development of cyberspace capabilities and training. Dr Jabbour expressed interest in the capability to use the Virtualized Intranet Platform for Exercise Realism (Chapter IX) in training young Air Force Reserve Officer Training Corps cadets during a summer program he conducts.

July 2007; Nellis AFB, NV: The information gleaned from the personnel at Nellis AFB was invaluable to this researcher. Mr Jim Hird heads the efforts of the Detachment 2 of the Air Force Information Operations Command in integration IO into the Flag exercises under the Air Warfare Center. Mr Hird provided insight into the efforts to develop Joint IO Range targets for Red Flag as well as visualization improvements to the Nellis Air Combat Tracking System. Blue Flag will begin to encompass more cyberspace threats because of inputs and initiatives led by Mr Hird. LtCol Reb Butler (57

المنارة للاستشارات
www.manaraa.com

IAS/CC) and LtCol Robin Williams (57 IAS/DO) are the conduit between the cyber warriors and the flying community at Nellis. They are bringing cyberspace into the mainstream at Nellis and have several efforts underway to integrate cyberspace effects into existing exercises, most notably Red Flag.

September 2007; Red Flag-Alaska, Eielson AFB, AK: The trip to Eielson AFB provided tremendous insight into the development of the Air Forces newest Flag venue. The interviews with Col Moore and LtCol Welch allowed this researcher a clear view of the differences between the existing Red Flag at Nellis AFB and Red Flag-Alaska. Eielson will not only provide training on par with Red Flag-Nellis, but also has tremendous potential to expand into areas, such as cyberspace, because it is a more isolated and focused environment. Nellis supports a tremendous number of missions and events with Red Flag being only a minor part of the overall operation. Eielson has the sole mission of supporting Red Flag, which enables tremendous potential for future training opportunities.

October 2007; MIT Lincoln Laboratory, Boston, MA: The trip to MIT Lincoln Laboratory focused on the potential of using the Lincoln Adaptable Real-time Information Assurance Testbed (LARIAT) to develop the Virtualized Intranet Platform for Exercise Realism (Chapter IX). Dr Rob Cunningham and Mr Lee Rossey were a tremendous help in developing a game plan for integrating LARIAT into a portable network environment to support Cyber Flag.

www.manaraa.com

Military Decision Making Process

The Military Decision Making Process (MDMP) provided this researcher a comprehensive framework of analysis to ensure the complete development of this research effort. This process, used extensively by the Army, provides the following steps in dissecting a problem:

1) Receipt of Mission
2) Mission Analysis
3) Course of Action (COA) Development
4) COA Analysis
5) COA Comparison
6) COA Approval
7) Orders Production
8) Rehearsal
9) Execution and Assessment

This researcher utilized steps 3-6 of the MDMP process to develop three COAs associated with the research question: ***Is there a need for a dedicated Flag focused on the employment of capabilities within cyberspace?*** As discussed previously, the research clearly and consistently showed the need for Cyber Flag and the following COAs are the suggested vehicles for this effort.

1) **COA 1:** The first option is to extend deployed forces for a one-week period after a Red Flag to support Cyber Flag.

المنارة للاستشارات

www.manaraa.com

2) **COA 2:** An alternate option is to create a network infrastructure like Bulwark Defender with nodes at Air Force bases with aircraft.

3) **COA 3:** The final option is to deploy forces for a dedicated Cyber Flag exercise in which the objectives support effects primarily focused on non-kinetic means.

Chapter VIII outlines and analyzes these COAs in accordance with steps 3-6 of the MDMP.

المنارة للاستشارات
www.manaraa.com

VII. Integration

> *"He who wants to protect everything protects nothing," is one of the fundamental rules of defense.*
>
> - General Adolf Galland

Every year there are new technological advances that provide more battlefield capabilities, but at ever increasing cost and complexity. Capabilities like Blue Force Tracking (BFT) and Fighter Data Link (FDL) transmit invaluable information between troops and airplanes using computer data links. A fighter pilot can instantly know who in his formation targeted an adversary, their weapons status, fuel state and other key concerns without even keying the radio microphone. Before FDL, pilots were lucky to communicate even a fraction of this information using radio transmissions over the constant radio chatter inherent to any moderately sized air operation. The same is true for the capabilities that BFT brings to troops in the field. Soldiers can determine instantly where members of their unit are despite darkness, terrain, weather, or distance. The enabling capabilities of BFT and FDL bring with them an inherent vulnerability. If data flowing through these networks is compromised or inhibited, operations will likely terminate at least temporarily because of the dependence on the information. Cyberspace enables the capabilities of FDL and BFT. Nevertheless, offensive action in this domain can just as easily take this ability away. As the realization of the significance of cyberspace begins to move into and through the senior Air Force leadership, there are increasing efforts to integrate these types of vulnerabilities into existing exercises.

المنارة للاستشارات
www.manaraa.com

Strategic Exercises

This researcher recently participated in Future Capabilities Games 07 at Maxwell AFB as lead planner for Red Team Cyberspace Operations. The Air Force Wargaming Institute hosted the six-day exercise on 14-19 October 2007. This was the first time in the game's eight-year history that cyberspace and information operations played a role. The Future Game exercise is a USAF Chief of Staff sponsored event, acting as a vehicle to guide future Air Force acquisition efforts (2027). The classification level of the game required the omission of the explicit results from this thesis. However, generically speaking, cyberspace operations played a crucial role in how the war played out. The significance of this fact cannot be over-emphasized. LtGen Robert J. "Bob" Elder, 8th Air Force commander and leader of the FG 07 Blue Team, eloquently communicated the increasing role that cyberspace must play in acquisitions decisions during his 19 October 2007 out-brief to Gen Duncan J. McNabb, USAF Vice Chief of Staff. This integration of cyberspace operations into Future Games is a seemingly insignificant event but represents the start of a much broader effort to bring cyberspace into the forefront of military thought.

Operational Exercises

> *"The start of the exercise accurately portrayed the 'chaos of war' as an early morning lightning bolt actually struck a building near the operations center just as players and controllers prepared to start the air campaign. Power and communications were temporarily disrupted as technicians brought backup power online and re-established network connections to controllers here. Within an hour, operations were restored and the simulated campaign continued."* [70]

المنارة للاستشارات
www.manaraa.com

This excerpt from the 2005 Blue Flag exercise could just as easily been the result of a computer network attack. Detachment 2 of the Air Force Information Operations Center (AFIOC) is responsible for integrating IO into the Air Warfare Center exercises, including Red Flag, Virtual Flag, and Blue Flag. In an interview with Mr Jim Hird, AFIOC Detachment 2, this researcher learned about many of the efforts underway to integrate cyberspace effects into operational exercises. The role of network attack and defense is increasing within Blue Flag. Exercise coordinators throttle this activity, however, to avoid conflict with the traditional exercise objectives, namely training those who operate the CAOC. As a result, these future IO integration efforts will likely fall short in achieving the effects through cyberspace that challenge exercise participants as much as natural conditions have previously done. A dedicated Cyber Flag exercise would prevent this from occurring.

Tactical Exercises

The boldest move toward integrating cyberspace operations into tactical training was the 30 January 2007 activation of the 57th Information Aggressor Squadron (IAS) under LtCol Reb Butler at Nellis AFB. The 57th IAS falls under the 57th Adversary Tactics Group (ATG) and is responsible for providing accurate threat replication of the cyberspace threat to tactical training audiences. By working closely with AFIOC Detachment 2, this squadron has made significant strides in the traditionally fighter aircraft dominated venues of the Air Warfare Center, most notably Red Flag. While there have been successes in the effort to present offensive cyberspace effects to the Red Flag audience, there are still significant challenges. As should be the case, there are limited

المنارة للاستشارات
www.manaraa.com

possibilities of demonstrating cyberspace effects without conflicting with the critical training that has been the vital focus of Red Flag for over 30 years. The primary drawback of integrating sophisticated information operations weapons, and other like capabilities, is that threats are often limited or removed from the Red Flag scenario that are critical to training young aircrew members. As discussed previously, Red Flag provides one of the few environments where aircrew can experience a robust surface-to-air missile threat. The White force personnel (responsible for administering the exercise) provide an insignificant subset of targets to non-kinetic capabilities so that their impact does not adversely affect the training of the participants. Plans are in place for wider use of the Joint IO range to increase targets for network attackers. Cyber Flag could be the ultimate answer to this critical objective by providing a robust set of credible cyberspace targets enabling the 57th IAS and information operations planners to exhibit the true capabilities of cyberspace to a Red Flag type audience. Although Red Flag and Bulwark Defender still provide key realistic training to aircrew and network defenders, what is now required is the combination of Bulwark Defender and Red Flag into an exercise emphasizing cyberspace effects achieved both kinetically and non-kinetically. The time is right for Cyber Flag!

المنارة للاستشارات
www.manaraa.com

VIII. Cyber Flag

> *The most important thing is to have a flexible approach. . . . The truth is no one knows exactly what air fighting will be like in the future. We can't say anything will stay as it is, but we also can't be certain the future will conform to particular theories, which so often, between the wars, have proved wrong.*
>
> - Brigadier General Robin Olds

Red Flag has evolved in very positive ways from its inception. Today, the exercise is less about training the young and inexperienced and more about large force employment in a robust threat environment. Red Flag must not lose sight of the importance of training Airman at all experience levels to employ in a joint/coalition force.

Our most likely adversary views the domain of cyberspace as the key to victory in future wars. Without our own parallel exercise venue, providing joint and coalition participants with a view into these enemy capabilities, development of adequate expertise and realistic training venues will continue at an unacceptably slow rate. As discussed in the previous chapter, the integration of IO capabilities into existing realistic training must continue. However, there should also be a dedicated exercise demonstrating offensive and defensive capabilities within air, space and cyberspace. A new Flag, Cyber Flag, could accomplish this broad objective.

Red Flag and Bulwark Defender independently provide key realistic training to aircrew and network operators but fall short in demonstrating cross-domain capabilities and effects. We now need the combination of Bulwark Defender and Red Flag into an

المنارة للاستشارات
www.manaraa.com

exercise, which emphasizes cyberspace effects, achieved both kinetically and non-kinetically. This Cyber Flag exercise would preserve the effectiveness of existing training venues while embracing the new domain of cyberspace, integrating capabilities drawn from across the services and coalition partners into one coherent effort. Bulwark Defender is a key exercise of joint defensive capabilities within cyberspace. Cyber Flag enables a training environment that integrates both offensive and defensive cyberspace effects into the mainstream operational and tactical planning effort. A Joint Force Commander for Cyber Flag would have the capability to call on IO options or capabilities as readily as a bomb or other kinetic weapon.

The development of such an environment is more palatable when divided into a three-year and 10-year vision, fully focused on maximizing exposure of participants to effects realized within cyberspace.

Three-Year Vision: *Best Practices and Realistic Scenarios*

A starting point for the establishment of Cyber Flag is to combine the best practices of existing training (both military and civilian) with the most realistic cyberspace threats and scenarios thus enabling a single exercise serving as a proof of concept for the future. The center of the Nellis AFB Red Flag exercise is the Nevada Test and Training Range (NTTR), providing approximately 1,000 square miles for participating aircraft to maneuver against realistic air and ground threats. Similarly, the center of cyberspace exercises is the Joint Information Operations Range, which provides an isolated network of geographically separated nodes capable of emulating a large number of real-world network topologies. The Joint IO range isolates cyberspace effects

المنارة للاستشارات
www.manaraa.com

from the public Internet while protecting tactics, techniques, and procedures from observation by potential adversaries. In addition, this range protects training events from external influences, thus providing a perfect foundation for the Bulwark Defender exercise. Similarities between the NTTR and Joint IO range environments, as well as the objectives of the Bulwark Defender and Red Flag exercises, provide an excellent starting point for integration. By adding the appropriate command and control infrastructure enabled by the Joint IO range, the defense of networks supporting a tactical exercise like Red Flag will become critical as aggressors attack them. The operational-level communications infrastructure exists as part of Bulwark Defender but lacks ties to the tactical-level planning effort. The objectives of Bulwark Defender are an important part of evaluating network defenses, however. We can now take training to the next level by utilizing the information flowing on the network to achieve tactical objectives. The fusion of the Bulwark Defender and Red Flag environments and scenarios, into a Cyber Flag exercise, allows aviators and network operators alike to see cyberspace effects played out in real-time. Because Cyber Flag would emphasize cyberspace effects, there is no conflict with existing training as would be the case if a network attack affected Red Flag flying training. Friendly network attack forces participating in Cyber Flag would play a critical role in attacking aggressor target arrays, also enabled by the Joint IO range. Vital to creating realistic cyberspace targets is the ability to replicate threat systems on the IO range which, when incorporated with the physical Cyber Flag target array on the NTTR, would create an integrated warfighting environment. Cyber Flag scenarios and lessons learned would then adjust to incorporate this enhanced capability. A technical

المنارة للاستشارات
www.manaraa.com

solution, which will provide assistance in this effort, is the Virtualized Intranet Platform for Exercise Realism (VIPER), defined further in the next chapter.

The visualization component of this integration will provide a significant challenge. The Nellis Air Combat Tracking System (NACTS) is the window into the Red Flag battle, but is not oriented toward demonstrating battlefield effects beyond the conventional realm. During post mission debriefings, the NACTS allows for repeated replay of the air war on huge screens so that the hundreds of participants have a true understanding of what transpired during the mission. Skillful use of debriefing slides will initially compensate for a lack of cyberspace effects visualization but there must be a future vision for a more robust capability displaying the real-time effects of the air and cyberspace battle. Until this type of capability exists, warriors will not fully realize the power of this new warfighting domain and how effects are the key to fighting and winning wars, rather than solely the attrition of target sets.

10-Year Vision: *Cutting Edge Dominance*

The next decade should focus on building Cyber Flag into a mainstream training exercise. With even a small-scale proof-of-concept for Cyber Flag realized in the near-term and a constantly improving visualization capability over the next several years, cutting edge dominance in cyberspace requires multiple large-scale annual events to maximize exposure to this critical training. The Cyber Flag transformation is very similar to the changes that EW brought to wafighting efforts, spawning the Green Flag exercise as discussed in Chapter I. The breadth and revolutionary nature of waging war in cyberspace extends beyond the goals and objectives of Red Flag and thus suggests the

المنارة للاستشارات

www.manaraa.com

need for a parallel approach. The realization of a cyber attack that brings all exercise operations to a halt would likely drive home the point that we are fighting a much different type of war. The goal of this type of exercise would be to demonstrate offensive and defensive cyberspace capabilities. This approach closely mirrors how the Chinese have trained since the late 90's in their transformation from a "mechanized PLA force to an informationalized force" [14]. As Timothy L. Thomas states in the book *Dragon Bytes*:

> *"In October 1999, the PLA conducted another IW exercise. Two army groups of the Beijing Military Region conducted a confrontation campaign on the computer network. Reconnaissance and counter reconnaissance, interference and counter interference, blocking and counter blocking, and air strikes and counter air strikes were practiced. The Operations Department of the General Staff said this was the first time that a computer confrontation was conducted at the campaign level between a red army and blue army. Actual field operations of a similar nature were conducted simultaneously in the Jinan Theater. According to one observer, the performance of the high-tech weaponry was like that of a 'tiger with wings.' The force demonstrated new tactics of using live ammunition to hit enemy cruise missiles and computer technology to hit information networks, links and points."* [14]

This excerpt is from 1999, the training and capabilities of the PLA have likely improved a great deal, due in part, to such credible training. Our future vision for realistic training should rise to meet this level of threat while breaking free of the geographic boundaries imposed by the current exercise arenas.

Most people in the Air Force are familiar with the Phase II employment exercise environment, which simulates that a base is under attack. Participation in a future Cyber Flag could have the same flavor, with a base required to launch attacks from home station while under attack from air, space, and cyberspace. Building on this premise, by 2018

www.manaraa.com

the realistic training environment should involve a widely distributed war involving multiple bases, conventional ranges, and computer networks. The continual growth of network and communication capabilities makes this a realistic prediction given the proper emphasis and planning. Unlike the evaluation model of a Phase II exercise, this exercise would provide training to participants just as Red Flag has done for years. What better test of training and preparation than an environment where operations are inhibited by e-mail server compromises, degradation of mobile and public switched telephones (or their successors), as well as assaults by aggressor aircraft? The Chinese see this type of training as the way to exercise kinetic and non-kinetic options by their informationalized force, as demonstrated in the above exercise report. In order to provide dominance within air, space, and cyberspace the US must do the same. The capability to experience such a robust combat environment at one's home station is the ultimate goal of realistic training since it enables the maximum amount of training using the most realistic forces in the shortest amount of time at the least expense.

Although it is difficult to even fathom what the world, much less the Air Force, will look like beyond the this 10-year vision, we must strive for a cyberspace capability equivalent to the *shock and awe* campaign of Operation Iraqi Freedom. In order to accomplish this, there must be a continuing effort to keep pace with technology and bring the realities of the cyberspace battlefield into our everyday operations.

Military Decision Making Process (MDMP)

Using the MDMP as outlined in Chapter VI, there are three viable Courses of Action for implementing the Cyber Flag exercise.

المنارة للاستشارات
www.manaraa.com

COA 1: The first option is to extend deployed forces for one-week after a Red Flag to support Cyber Flag. Table 6 provides a sample flow for the week. As an example, participants would see a Thailand threat with capabilities focused on benign network scans searching for system vulnerabilities. If Thailand has technology that allows for the search for vulnerabilities outside IP-based networks (such as closed battlefield or airborne linked systems) then scanning of these systems could take place as well. If not patched, these vulnerabilities provide the foundation for attacks on networks during the future days of the exercise. The goal would be for participants to recognize and counter this scanning activity if possible. Offending network nodes and systems, if positively identified, could become potential targets for future day's missions.

In addition, the following the threat levels provide a graduated learning environment as follows:

- Level I: Benign Target
- Level II: Defended Target
- Level III: Aggressive Target (i.e. shoots back)

These threat and target types represent the focus for operational planning and tactical employment during the week of Cyber Flag. The networks supporting the operational planning would be subject to the effects listed in Table 6, given the type of vulnerabilities that exist. The CAOC would be under constant attack and ATO production must continue to fuel the tactical missions. If it were impractical to have the Nellis CAOC attacked, then a notional CAOC tied to the Joint IO range would produce products in parallel with those used to fly actual missions.

المنارة للاستشارات
www.manaraa.com

Table 6 Cyber Flag Scenario Matrix

Day	**M**	**Tu**	**W**	**Th**	**F**
Threat	Thailand	India	Russia	China	China
Level	I	II	III	III	III
Types	C2	C2 & SCADA	C2 & SCADA	C2&Airborne	All
Vulnerability	Patches	Patches & Protocol	Patches & Protocol	Phishing, Virus Worm	All
Effect	Scans (IPB)	Scans & Hooks	Web Page Deface, Anomalous Activity	Data Extraction, DOS, EA	All

Mission planning could ensure target pairing to both kinetic and non-kinetic capabilities.

Pros: This option would preserve existing Red Flag training objectives accomplished during the previous week's missions. The cyberspace domain would be the emphasis of the additional week of training. This is an optimal scenario because it allows a robust Air Expeditionary Force to employ against the most realistic threat while focusing on the enabling effects within cyberspace.

Cons: Funding for unit deployments would have to be increased but costs compared to deploying and redeploying the necessary forces are minimal.

COA 2: A second option is to create a network infrastructure like Bulwark Defender with nodes at Air Force Bases that have aircraft. Table 7 provides a suggested force structure and associated participants. Aggressors would conduct network warfare against the operational command elements of the network while Blue Forces task aircraft to provide tactical support.

www.manaraa.com

Table 7 Distributed Cyber Flag Players

Squadron	Role	Base
1st Fighter Wing (F-15 / F-22)	Offensive Counter Air / Red Air	Langley AFB, VA
ACC NOSC / INOSC	Command and Control	Langley AFB, VA
2nd Bomb Wing (B-52)	Interdiction / Strike	Barksdale AFB, LA
AFNOC	Command and Control	Barksdale AFB, LA
8th AF	CAOC	Barksdale AFB, LA
33 IOS	Net-D	Lackland AFB, TX
315 IOS	Net-A	Ft George Mead, MD
355th Wing (A-10)	CAOC / CAS	David Monthan, AZ
SOCOM	CAOC	Hurlburt AFB, FL
57 IAS	Information Aggressors	Nellis AFB, NV

In addition, aggressors would implement elements of CNA, CND, PSYOPS and EW at the tactical level by targeting base-level communications infrastructure.

Pros: This would be the lowest cost option for Cyber Flag because bases could support the exercise without the deployment of aircraft. The aircraft could also fly alternate missions if the cyber effects prevented them from executing the primary tasking. A base-level exercise would also exhibit a broad range of cyber effects to a very diverse audience including communications, maintenance, aviation, and security police personnel. Jamming could take place against cell phones and land mobile radios. Internet attacks could start with propaganda via web pages and phishing attacks aimed at gaining network access. The escalation of the exercise could then see complete denial of service attacks against networks on base similar to an “Alarm Black” type event during a Phase II.

Cons: This would require base-level participation similar to a Phase II exercise. Nearly all base operations would cease except those supporting the exercise.

المنارة للاستشارات
www.manaraa.com

COA 3: The final option is to deploy forces for a dedicated Cyber Flag exercise in which the objectives support effects based primarily on non-kinetic means.

Pros: There is nothing better than a dedicated venue for highlighting the enabling capabilities of cyberspace. The benefit of this COA over COA 1 is the emphasis on cyberspace. If participants extend their stay after Red Flag to participate in Cyber Flag there is potential for a deemphasized approach. This COA is the remedy for that problem.

Cons: The lack of money available to spend on additional training or to upgrade existing training is a growing concern. There will have to be a tremendous reprioritization of funding for training and programs to enable this type of Cyber Flag. This researcher recommends careful consideration of funding priorities based on the most likely threat and future warfighting environment.

المنارة للاستشارات
www.manaraa.com

IX. Virtualized Intranet Platform for Exercise Realism

> *If you build it, they will come.*
>
> - Kevin Costner (Field of Dreams, 1989)

One of the most crucial elements in implementing the Cyber Flag CONOPS is to provide the capability to turn nodes of the Joint IO Range into either blue networks (for defense) or red networks representing blue target sets. The idea behind the Virtualized Intranet Platform for Exercise Realism (VIPER) is that a portable network replication suite provides required capabilities at a minimal cost. Remote access to VIPER, enabled through an IP-managed keyboard-video-mouse (KVM) switch, also reduces cost by minimizing the need for on-site maintenance personnel.

This chapter provides an overall outline for implementing a simulated network and traffic generation capability in support of Cyber Flag. This environment uses the Lincoln Adaptable Real-time Information Assurance Testbed (LARIAT) developed by Lincoln Laboratory. The 346th Test Squadron at Lackland AFB, TX currently uses the LARIAT software suite successfully.

Synopsis

VIPER uses VMware and LARIAT to simulate up to three Air Force Base networks. The utility of this environment serves four key purposes:

1) Provide an academic learning environment for the capabilities of the LARIAT network including:

www.manaraa.com

    a. Traffic generation
    b. Network replication
    c. Internet simulation

2) Hardening of networks constructed for other purposes within the academic environment at the Air Force Institute of Technology (AFIT).
    a. The annual Cyber Defense Exercise (CDX) can bridge to VIPER, testing usability and security.
3) Development of VIPER can act as a target for offensive network activities. The AFIT network attack classes can utilize VIPER for a more realistic representation of a target network.
4) Finally, the VIPER provides a portable network replication node for integration with the JIOR. This replication environment allows for defensive training on a base network or provides a target for network attacks.

Hardware Requirements

As mentioned previously, the 346th has demonstrated the practicality of the LARIAT environment. This realism, coupled with portability, makes VIPER (depicted at Figure 5) an excellent building block network to support Cyber Flag. Using virtualization technology, the ability to replicate hardware using software, VIPER provides a small-scale network with simulated users and acts as either a target of computer network attack or a defensive training platform.

VIPER is self-contained and portable with the ability to connect to a larger training network like the Joint IO Range. The basis for the network replication is

المنارة للاستشارات
www.manaraa.com

LARIAT [65]. The LARIAT software links virtualized Air Force Base networks with simulated users to provide a realistic environment for training in network attack or defense. Table 8 summarizes the hardware costs associated with VIPER. VMware Server 1.0.4 provides the virtual network framework including the appropriate operating system and network services.

Table 8 VIPER Hardware Costs

Component	CPU	RAM	Hard Disk	Cost
Dell Power Edge 860 Server	Dual Core 2.4GHz	4GB	80GB	$2506.03(x5)
Laptop	Dual Core 1.5GHz	2GB	250GB	$999.00
Cables	10' Cat-5 Patch Cable (x10)			$104.30
Switch	12 Port Switch (CISCO 2950)			$549.99
Router	Cisco 2600 Single Interface Router			$578.75
KVM Switch	Avocent Autoview 1000R IP Managed KVM			$2718.04
Case	8 Server Transportable Hard Case			$1023.42
Optional Items	Monitor, Keyboard, Mouse, 500GB External Hard Drive			$500.00
Total				$19,003.65

The LARIAT package provides the capability to emulate user activity on the virtual Air Force Base networks. VIPER consists of five servers linked by a 12-port switch (Cisco Catalyst 2950) with an additional laptop connected for system management (Figure 5). A single interface Cisco 2600 router allows routing within the network environment. The five-server model provides large enough networks for training but scales to much more complex hardware configurations as required. One Dell Power Edge 860 server hosts the LARIAT traffic generation server, providing traffic within and

المنارة للاستشارات
www.manaraa.com

between each of the three AFB networks. Another Dell server provides a simulated Internet environment including the ability to access popular web pages such as ESPN.com and CNN.com.

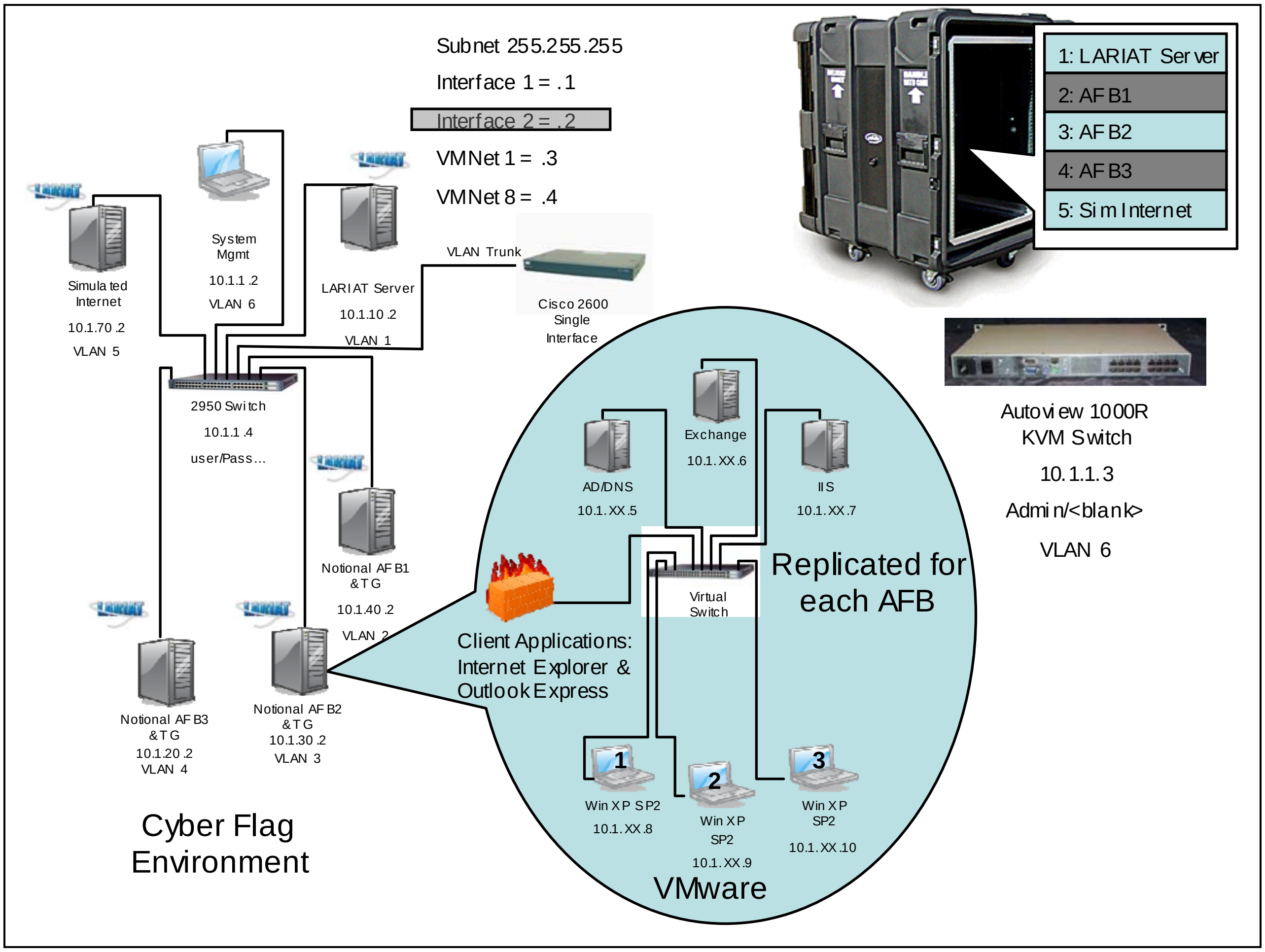


Figure 5 Virtualized Intranet Platform for Exercise Realism (VIPER)

The traffic generator enables virtual users with accounts on each base network to access web pages, within each base and the simulated Internet, as well as the ability to send and receive e-mail. The remaining three Dell servers support the virtualized Air Force Base networks. Each of these base networks contains three clients, with multiple

المنارة للاستشارات
www.manaraa.com

user accounts, and three servers, providing Active Directory, Domain Name, Exchange, and Internet Information Server services. This architecture is very simplistic yet serves as a baseline proof of concept for a much larger physical and virtual network. LARIAT can support a large number of operating systems and applications, making it relatively easy to expand to models that are more robust. As an example, VIPER consists of Microsoft Windows based networks using Windows Server 2003 Service Pack 2 for each server and Windows XP Service Pack 2 for the clients. LARIAT supports the full range of Windows operating systems as well as most versions of LINUX. In addition, VIPER initially supports Internet Explorer and Outlook Express applications but LARIAT allows virtual users to utilize a much broader range of applications such as the Firefox web browser and the full Microsoft Office suite. If the LARIAT software supported more applications inherent to the CAOC, the result would be an even more robust network defense platform.   The physical servers can support approximately three virtual servers and up to four virtual clients based on 4GB of memory and 80GBs of disk storage, each Power Edge 860 has two 80GB mirrored hard drives. Each virtual machine utilizes 10GB of drive storage and roughly 500MB of memory. By simply increasing the disk storage capacity and memory on the associated servers, much larger virtual network configurations are possible. According to Lee Rossey, the lead developer for LARIAT, Lincoln Laboratory routinely runs 30 virtual machines on servers using machines with equivalent processor capacity to those supporting the VIPER model, 16GB of physical memory, and 350GB of hard disk storage.

www.manaraa.com

A laptop allows off-site system monitoring and control of VIPER using the Avocent KVM switch and the *What's Up Gold* network mapping application (Figure 6 and 7).

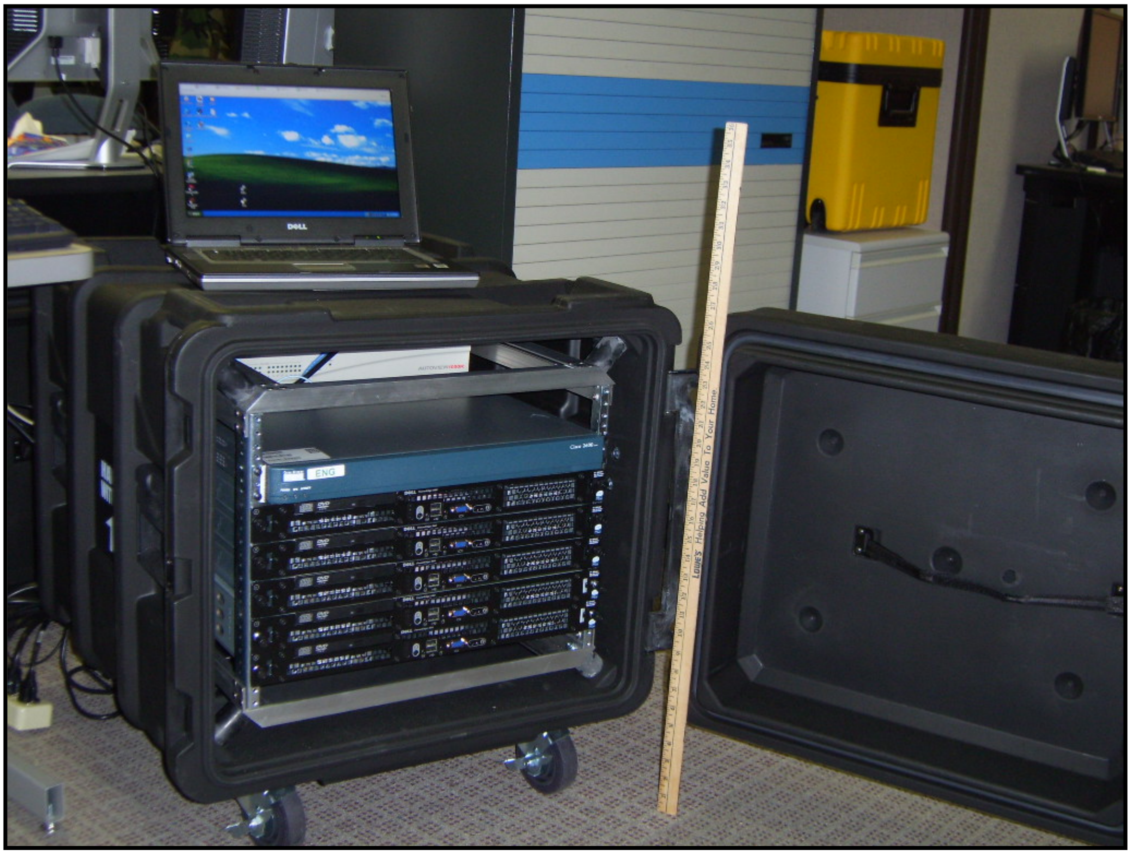


Figure 6 Prototype VIPER Node

Software Requirements

The LARIAT software package provides a capability to both replicate Windows networks and to simulate user activity on those networks. The LARIAT Tenets are [65]:

1) Provide traffic modeling
    a. Emulate user actions and activities
    b. Configurable traffic patterns and flows
2) Provide tools to assist operators in constructing a network attack range

المنارة للاستشارات
www.manaraa.com

a. Automation of services

b. Connectivity testing

3) Provide tools to test situational awareness and analysis

a. Monitor traffic and machine health

In keeping with these objectives, LARIAT is constantly evolving based on user requirements and technological advances. By their own testimony, the Lincoln Lab team is more than willing to add user models, applications, and other features to LARIAT that will expand its capability and user base. With this in mind, the ability to provide a simulated CAOC for defensive training, or the enemy equivalent, is not beyond the scope of reality.

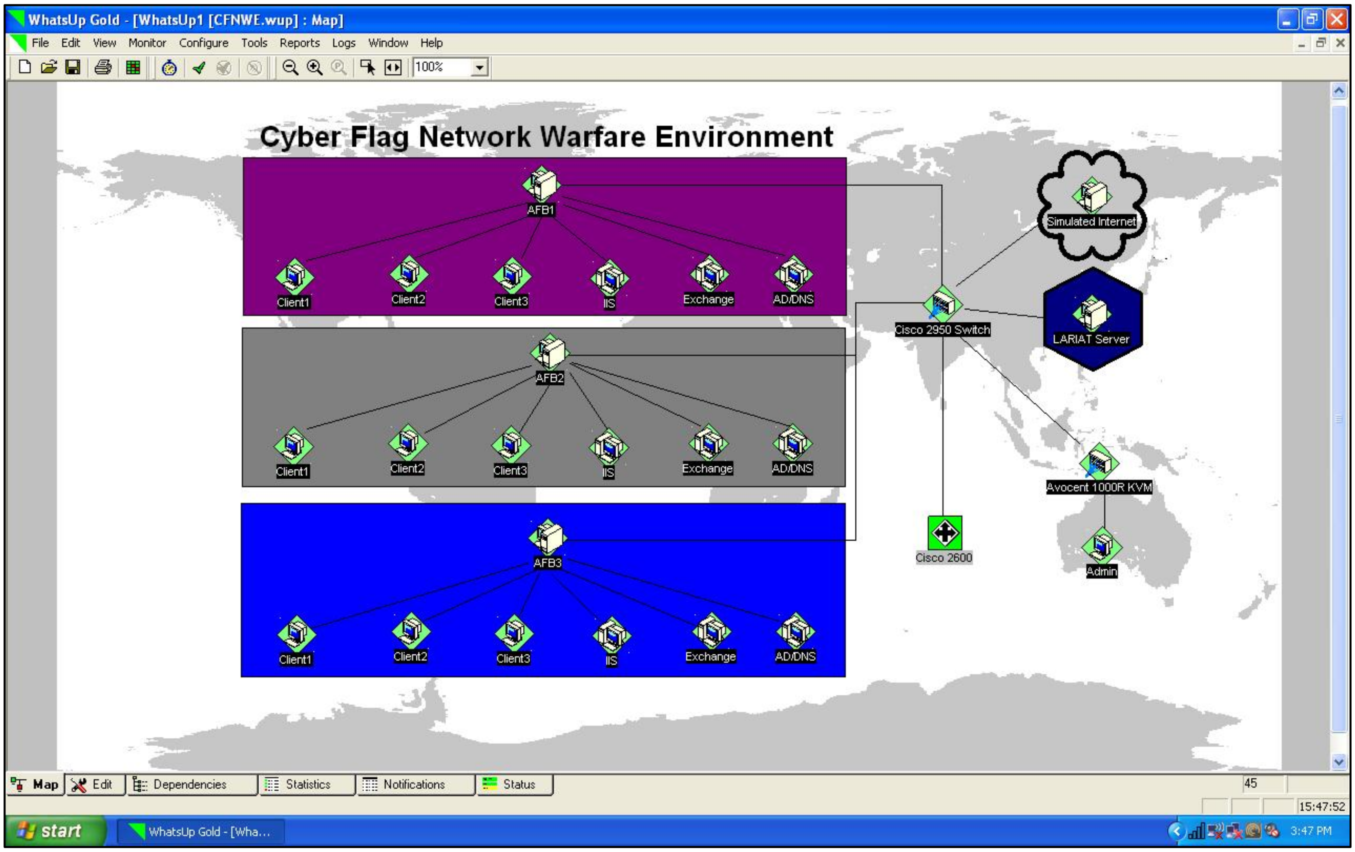


Figure 7 VIPER Network Mapping

www.manaraa.com

Summary

VIPER provides a robust learning environment for AFIT in addition to an expandable proof of concept for the Cyber Flag CONOPS. The design of the system combines portability and cost efficiency to enable a building block for wide-scale integration on the JIOR. In addition, the system can be remotely managed thus requiring low manpower for support and operation in the field. All of these elements combine to allow widespread implementation immediately.

المنارة للاستشارات
www.manaraa.com

X. Results and Conclusions

> *I would not give a fig for the simplicity this side of complexity, but I would give my right arm for the simplicity on the other side of complexity.*
>
> \- Oliver Wendell Holmes

The following key questions emerged during this research effort and the answers provided insight into the future course of realistic training.

1) **How have the current Flags and Exercises evolved to address changing defensive threats and offensive opportunities largely driven by technological changes?** Chapter IV, Chapter VII, and Appendix A address the evolution of realistic training exercises at the strategic, operational, and tactical levels of war. A constant theme in these efforts is the conflict between implementing new elements of exercises and the existing training objectives. There have been several instances of new exercises, most notably Green Flag, generated with the sole purpose of maintaining current and necessary training objectives while highlighting a fundamental warfighting capability.

2) **How do we visualize effects within cyberspace in conjunction with kinetic effects during the course of an exercise?** Chapter V, Chapter VIII, and Appendix B address the lack of visualization technology in-place today. There is significant work underway to enable a visualization capability but funding priority issues have limited this effort [40]. In addition, a lack of funding has delayed or cancelled many of the upgrades to the NTTR that will

www.manaraa.com

realistically reflect the battlefield of tomorrow. The majority of the threats on the NTTR cannot replicate modern-day surface-to-air missile systems or the advanced command and control capabilities of our adversaries. Funding has also limited the development of an effect-based visualization capability for Red Flag participants [40]. Without an environment that accurately reflects NCW, EBO, and cyberspace, the training effectiveness of the aggressors is diminished.

3) **Who are the key threats operating within cyberspace and how are they training?** Chapter II fully addresses the broad range of threats that operate within cyberspace including terrorists, hackers, crackers, and nation-state actors. Although China represents the baseline threat within cyberspace, based on their expertise and emphasis on Information Warfare, they are by no means the most likely adversary. The capability to continue to refine the most capable and likely threats with the cyberspace domain is left as a significant challenge for the Intelligence community. The capability to characterize current and future adversaries will be critical in the development of offensive and defensive cyberspace operations as well as realistic training.

4) **How do we plan and coordinate information operations in conjunction with conventional operations to mitigate defensive threats and provide offensive opportunities within cyberspace?** Chapter V addresses current IO planning within cyberspace as well as future requirements for weaponized capabilities. There are increasing efforts to integrate IO with conventional

للاستشارات المنارة
www.manaraa.com

operations stemming from the activation of a Major Command focused on cyberspace and the accompanying force development effort. With a refined cyberspace force, comes the inevitable guidance on the roles and missions associated with that force as well as a formal tasking process. Once accomplished, a clear understanding of offensive opportunities in cyberspace can be established inside the USAF with eventual widespread use of those capabilities both within the Air Force and DoD.

5) **What initiatives are underway to integrate cyberspace effects into existing Flags and exercises?** Chapter VII identifies current integration efforts. The consistent theme identified in this chapter is the conflict that exists between current critical training objectives and the integration of cyberspace capabilities. Cyber Flag provides a solution to this conflict, providing a realistic training environment in order to evaluate the threats and required capabilities within cyberspace.

6) **Is there a need for a dedicated Flag focused on the employment of capabilities within cyberspace?** Chapter VIII provides an explanation for the need to develop a dedicated cyberspace exercise, Cyber Flag. The fiscal and force structure limitations require tough choices between existing weapons and training programs and the much needed emphasis on cyberspace. Cyber Flag represents the most cost effective alternative to optimize existing resources while providing the required emphasis on the cyberspace mission area.

المنارة للاستشارات
www.manaraa.com

Implications

This research provides an evolutionary approach to integrating cyberspace capabilities into existing exercises and defines a Concept of Operations (CONOPS) for Cyber Flag (Appendix C). The intent is to provide guidance to existing Air Warfare Center and Air Combat Command staff members guiding the fundamental evolution of realistic cyberspace training.

Results

The CONOPS for Cyber Flag was presented to the 57 ATG Commander, Col David Stilwell, who is charged with developing the way ahead for Red Flag for MajGen Warden the AWFC Commander. Col Stillwell considered the Cyber Flag concept viable but funding limitations restrict implementation. There should be a further discussion regarding the prioritization of funding based on current training objectives and the future threat.

Conclusions

The time is right for Cyber Flag given emerging technology, a pervasive threat, and the conflict with existing exercise objectives. As is commonly understood, there is no better training than the hands-on realism associated with participation in an exercise such as Red Flag or Bulwark Defender. Secretary Michael W. Wynne has a vision for dominant operations in cyberspace "comparable to the Air Force's global, strategic omnipresence in air and space" [17]. This vision requires a combination of joint coordination, skilled forces and a realistic training environment to bring them all

المنارة للاستشارات
www.manaraa.com

together. Budget constraints and a failure to accept cyberspace as a decisive warfighting domain could put the United States military in a poor position against future enemies. Cyberspace increasingly stitches together the diplomatic, information, economic and military instruments of power. The creation of a dedicated Cyber Flag exercise allows the preservation of critical learning objectives of current exercises while preparing forces to understand the important role of cyberspace in achieving battlefield success. The United States military does not currently have an advantage in cyberspace and the future of our nation depends on the military's ability to harness the best practices to achieve cutting-edge dominance and ultimately shock and awe within cyberspace.

Future Research

Given these results, the following areas require future research:

1) Explore the utility of expanding the hardware and software capability of LARIAT to enhance the training environment. Although the VIPER provides a starting point, the reality of technical advance makes this an iterative process. One example would be to upgrade the software capabilities of VIPER using VMware ESX. There is a free academic license available for VMware ESX and future development of VIPER would benefit greatly from its use. The VMware ESX software acts as a host operating system as well as managing all of the virtual machines created. This eliminates the memory and processor overhead associated with having VMware act through a host operating system (currently Windows Server 2003 for VIPER) which in-turn increases performance. This researcher estimates double the number of

المنارة للاستشارات

www.manaraa.com

virtual machines for each physical VIPER server with the use of VMware ESX.

2) Conduct a broader look into service-level training requirements and provide recommendations on redundant training exercises. These redundancies provide ways to both consolidate training and to free up funding for a dedicated Cyber Flag initiative.

3) Develop scenarios for use with VIPER that will assist in the network attack and defense education and training process. VIPER provides a robust capability to allow for both offensive and defensive training. These scenarios would require trainees to shore up network defenses of VIPER to protect information from compromise. In addition, mission planning and attacks on VIPER validate tactics, techniques, and procedures of those trained for network attack roles. Phishing, keylogger, privilege escalation, and data mining are just some of the attacks realistically supported by VIPER. The resilient nature of VIPER allows rapid rebuild and repeat of scenarios, maximizing training for all involved.

4) There should be significant effort to enhance the capabilities of LARIAT for modeling of applications specific to the CAOC. Such efforts will significantly enhance credibility and training realism. Mr. Chris Connelly at Lincoln Labs is looking for assistance in developing these applications and this would be a very beneficial area for an AFIT student with CAOC experience to provide support.

المنارة للاستشارات
www.manaraa.com

5) Although this research recommends three COAs, there must be consideration for what happens beyond this near term view. Cyber Flag emphasizes cyberspace effects in order to jump start realistic training in this domain. An eventual outcome of Cyber Flag would be that streamlining of kinetic and non-kinetic operations eliminates conflicts with other existing exercise objectives. When this occurs, more cyberspace capabilities become part of exercises like Red Flag and Blue Flag until the need for Cyber Flag no longer exists. This was the fate of Green Flag as discussed previously. The development of a future vision that describes how Cyber Flag becomes an exercise that no longer just emphasizes cyberspace capabilities but more truly represents total war in all domains has significant utility in the mind of this researcher.

Cyber Flag is just the beginning of a broader effort to integrate cyberspace operations into mainstream military planning and execution. The VIPER is a building block for constructing a robust and comprehensive future training environment. We must start somewhere and VIPER provides that initial low cost training alternative that will start the iterative process of building the most capable air, space, and cyberspace force in the world.

المنارة للاستشارات
www.manaraa.com

Appendix A – Exercise Primer

This appendix contains reference material from AFDD 2-1 and other sources defining realistic training for the Air Force.

Red Flag

The history of Red Flag dates back to the end of the Vietnam War. Project Red Baron I and II were based on a series of studies including the evaluation of 400+ air-to-air engagements in Southeast Asia starting in 1967 [62]. The goal was to identify the root causes for the low (2.5:1) enemy vs. US fighter aircraft kill ratio achieved in Vietnam compared to the 10:1 kill ratio in Korea. In response to this analysis, the report highlighted the following [62, 8]:

1) There was a lack of Air Combat Maneuver (ACM) training across Air Force fighter units. Fighter crews lacked familiarity with enemy tactics and the maneuvers that could counter them.
2) The first ten missions during combat operations were the most critical for survival. Pilots with at least this number of sorties stood a significantly higher chance of survival.
3) Crews trained primarily against one another during peacetime training missions and, therefore, were not prepared to identify and counter dissimilar aircraft. As a result, nearly 80 percent of air-to-air losses were due to unseen adversaries. The Vietnamese Mig-17s and 21s were nearly half the size of the F-4 and F-105 [19].

المنارة للاستشارات
www.manaraa.com

One of the primary outcomes of the Red Baron I and II Reports was the establishment of the *Readiness through Realism* initiative sponsored by Tactical Air Command [8]. This initiative resulted in the following training improvements:

1) The Air Force generated four aggressor squadrons (64th, 65th, 527th and 26th) flying the T-38 and then the F-5 to provide dissimilar training.
2) In 1975, the Coronet Real program developed realistic target arrays and threat simulators [20].
3) The development of a robust suite of assessment tools, including optical scoring and SAM video debrief reconstruction using the Air Combat Maneuvering Instrumentation (ACMI) aircraft tracking system.

In addition, the specification of a Designed Operational Capability (DOC) [21] identified a primary and secondary mission for each squadron. This allowed squadrons tasked primarily to do air-to-air to dedicate the majority of their training sorties to this purpose.

The Birth of Red Flag

In April of 1975, the Directorate of Operations, Headquarters Air Force, provided a Concept of Operations (CONOPS) briefing for an exercise called Red Flag to attendees of the Fighter Weapons Symposium [15]. The CONOPS encapsulated the *Readiness through Realism* mindset into a single exercise providing the most realistic training environment possible for aircrews [15]. This environment intended to replicate the first ten combat missions to increase aircrew survivability in real combat. The Air Force Chief of Staff approved the concept on 15 July 1975 and the first Red Flag began on 27

المنارة للاستشارات
www.manaraa.com

November 1975 [15]. Participants consistently praised Red Flag (with subsequent results substantiating their effectiveness), resulting in the creation of similar exercises to provide realistic training in other critical areas.

Current Initiatives

The evolution of Red Flag over the past 30 years includes the addition of Combat Search and Rescue (CSAR), Dynamic Targeting (DT) and advanced Command, Control, Intelligence, Surveillance and Reconnaissance (C2ISR). Several changes over the past four years have further transformed Red Flag and its goal of cutting edge realistic training.

Aggressors

While the USAF Aggressor program began in 1972 and eventually grew to four full squadrons of F-5s, 1990 started a cutback that relegated the program to a small number of F-16s primarily supporting Red Flag. The Air Force Chief of Staff called for a resurgence of the Aggressors starting in 2003 with the 64th Aggressor Squadron reactivated in October 2003 with eleven F-16s and the 65th Aggressor Squadron activated in January of 2006 with seven F-15s at Nellis AFB [22]. In March of 2006, the Alaskan Cope Thunder exercise became *Red Flag-Alaska* with the traditional Red Flag designated *Red Flag-Nellis*. The 18th Aggressor Squadron activated August of 2007 with 22 F-16s at Eielson AFB to provide dedicated adversary support for *Red Flag-Alaska*. By providing two Red Flag venues, more units can be included in Red Flag in preparation for their respective Air Expeditionary Force (AEF) deployments.

المنارة للاستشارات

www.manaraa.com

57th Adversary Tactics Group

In June 2005 the 57th Adversary Tactics Group (ATG) activated at Nellis AFB becoming "Threat Central" for the Air Force [22]. The ATG added Space and Cyberspace Aggressors to the traditional air-breathing arsenal, bringing the 527th and 26th Space Aggressor Squadrons under its umbrella. In addition, a portion of the 92nd Information Aggressor Squadron (IAS) at Lackland AFB became the 57th IAS at Nellis AFB.

Green Flag

General Wilbur L. “Bill” Creech developed the Green Flag in 1978 to integrate the enabling capabilities of EW into realistic training. This exercise focused on signal intelligence and offensive EW platforms to highlight the necessity of these capabilities in the presence of a robust surface-to-air missile environment. These same capabilities are now a part of Red Flag and in 2006, the role of Green Flag dramatically changed. The Green Flag exercise now tests the air support of Army troops conducting battlefield exercises at The National Training Center (NTC), at Fort Irwin, and the Joint Readiness Training Center (JRTC) at Fort Polk. More specifically, Green Flag absorbed the exercise formerly known as Air Warrior I (now Green Flag-West) and Air Warrior II (now Green Flag-East) [49].

Blue Flag

The Tactical Air Command developed the Blue Flag exercise in 1977 to provide realistic training to CAOC staff members [50]. The CAOC is a weapons system and as

المنارة للاستشارات

www.manaraa.com

such requires great proficiency from those who operate it, as well as a dedicated Flag to provide a realistic training environment to develop this expertise.

Virtual Flag

The Virtual Flag exercise utilizes the ever-increasing capability of computer simulation to provide a realistic USAF training environment across the United States. The Distributed Mission Operations Center (DMOC) and the 705th Combat Training Squadron host this exercise [51].

> *"Think of Virtual Flag as a huge simulation in which our aircrews, space warriors and ground operators in the Air Operations Center, Control Reporting Center and Patriot missile batteries 'fight' the enemy completely in a virtual reality environment," Lt. Col. Gordon Phillips, 705th Exercise Control Squadron Commander* [51]

Because of the dramatic improvements in the intensity of the virtual environment, including the ability to pause the action, the Virtual Flag exercise allows every training objective to be covered [51]. Given the relatively small number of simulators, however, this training is only available to a very limited number of participants. Future expansion of Virtual Flag could create an environment on par with Red Flag in terms of the number of aircrew members trained. The benefits of this environment are incredible, in that, the scenarios do not have to be scaled-back to compensate for physical airspace restrictions or safety, as is so often the case today in Red Flag.

JEFX

The Air Force Experimentation Office (AFEO) stood up on January 1, 1999 to grow and administer a series of Joint Expeditionary Force Experiments (JEFXs)

المنارة للاستشارات
www.manaraa.com

exploring emerging technologies, tactics and requirements and enhance Air Force capabilities [54]. Held every two years, these experiments have come to represent the most comprehensive combination of live fly and simulation technologies using effects based operations. The JEFX is a unique environment developed to explore processes in a large and realistic net-centric environment. The results of these experiments allow Joint, DoD and coalition partners to realistically identify, analyze, and plan for future modernization decisions.

Experiments vs. Exercises

The experimentation process is fundamental to the way the Air Force evolves but its environment differs significantly from a training venue. Exercises exist to train forces while experiments give insight into the validity of future investments. The JEFX is not a classical scientific experiment but more of a concept demonstration environment.

Terminal Fury

This US Pacific Command exercise began October 2002 to test the contingency response of the Joint Task Force 519 [55]. This is an operational-level planning exercise, similar to Blue Flag, encompassing joint and coalition partners.

USAFWS Mission Employment Phase

The USAF Weapons School syllabus culminates in a one-week capstone phase called Mission Employment. This weeklong training focuses on student learning, within a multi-platform environment, to plan and execute a small-scale air campaign. The missions are roughly half the size of a Red Flag but involve much more highly trained

المنارة للاستشارات
www.manaraa.com

and experienced participants. The objectives are to push the limits of large force tactics, techniques, and procedures.

Maple Flag

The Maple Flag exercise was born out of Red Flag when in 1977 the Canadian Commander of Air Command invited the United States to hold a northern exercise in Cold Lake, Alberta [56]. This exercise uses the Cold Lake Air Weapons Range, which is similar in size to the NTTR but lacks the terrain and robustness of enemy defenses at Nellis AFB. The Maple Flag exercises tend to have a wider range of international participation when compared to Red Flag, with scenarios geared toward employment as a coalition force. The Mission Commander at Maple Flag is just as likely to be from an Allied nation as from the US with adversary forces traditionally led by the USAF Aggressors.

Northern Edge

The Northern Edge exercise has evolved from a cold climate training exercise to a robust multi-agency test of Alaska's homeland defense plan. The Jack Frost exercise, set in motion in 1975, followed by Brim Frost and Arctic Warrior through the 80's and early 90's, trained forces in arctic and winter environments. Northern Edge began in 1993 as a Joint exercise focused on operational command and control of the Alaskan Command [57]. The exercise evolved into the most recent venue, Northern Edge 2006, which incorporated 5,000 personnel, 110 aircraft, a Carrier Air Wing, and two Navy destroyers

المنارة للاستشارات
www.manaraa.com

[57]. This is one of the few exercises combining the Army, Navy, Marines, and Air Force in a homeland defense scenario with air, land, sea and space domains exploited.

المنارة للاستشارات
www.manaraa.com

Appendix B – Cyberspace Primer

This appendix provides additional background on the definition and models used to define cyberspace.

Models

There has been a great deal of work done in the area of modeling the cyberspace domain. If you can accurately depict cyberspace using a diagram, the likelihood of someone understanding increases markedly. During the course of this research effort, several models stood out as good representations of cyberspace.

It is important to understand that in a net-centric environment, the flow of data and information through cyberspace provides a capability to link specific network nodes. A “node” could be a computer, aircraft, person, or a multitude of other devices. The models at Figure 8-11 provide varying depictions of cyberspace. The Woolley Model, Figure 8, shows the interaction of data and information within cyberspace as the glue that ties together the physical, cognitive, and cyber domains. The Franz B-21 Model, Figure 9, represents the physical and cognitive domains as spheres encompassed by the information domain. Finally, the Wong-Jiru and Mills Model, Figure 10, depicts layers of networks with the information providing linkages between them. By combining elements of these three models, this researcher provides the model at Figure 11 as a way to highlight what is effective within each of the previous illustrations of cyberspace. This model represents the layering of networks with the associated linkages all encompassed by the information domain. Information can flow through the physical network linkages within a layer, or between layers through the cyberspace surrounding the nodes (e.g., the

المنارة للاستشارات
www.manaraa.com

electromagnetic spectrum). Using this amalgamated model, Figure 11 also depicts the cyberspace domain as surrounding networks within a battlefield environment. This is a baseline for representing the scope of this thesis in terms of a realistic training environment for cyberspace. The Figure 11 model depicts where attacks on network nodes or linkages between those nodes achieve effects within the physical or cognitive domains. The ultimate goal is to affect the top layer decision-making process so that the Observe, Orient, Decide, Act (OODA) process is inhibited for the enemy and protected for blue forces.

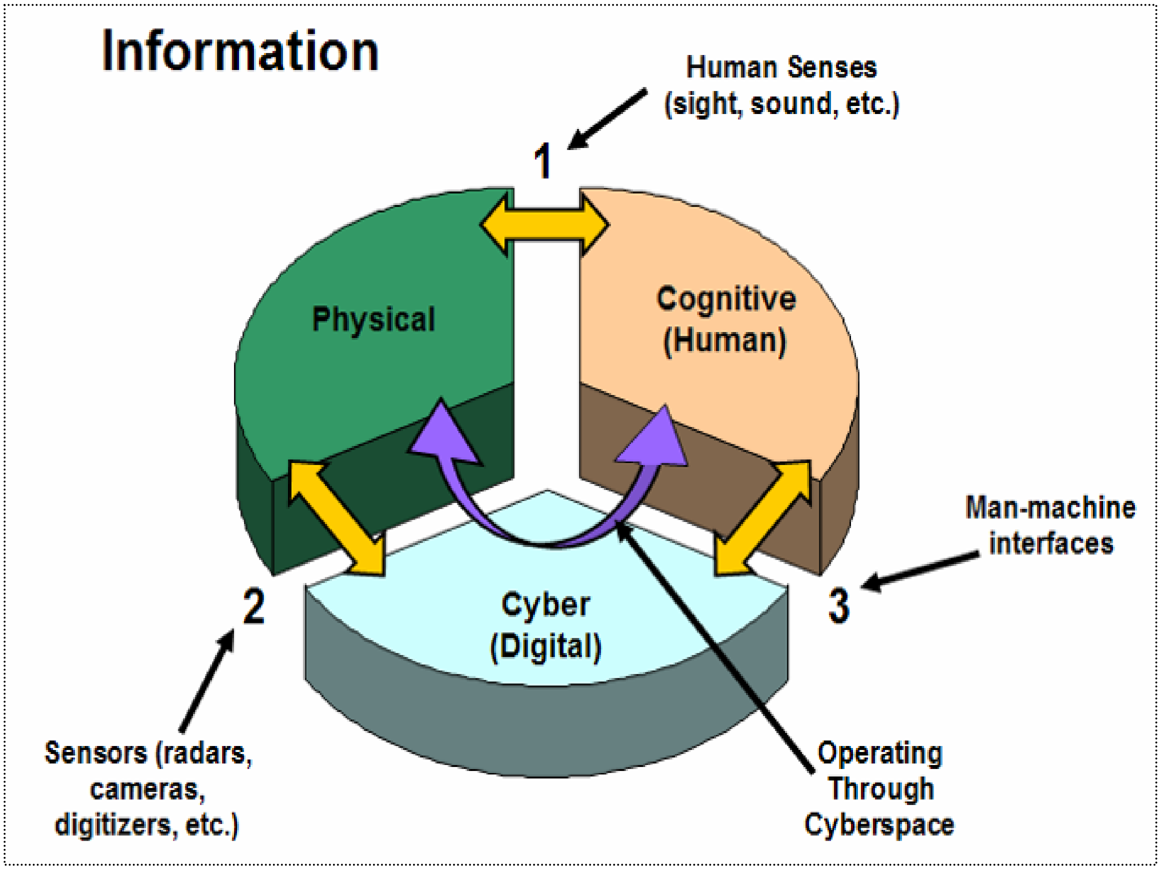


Figure 8 Woolley Cyberspace Model [58]

www.manaraa.com

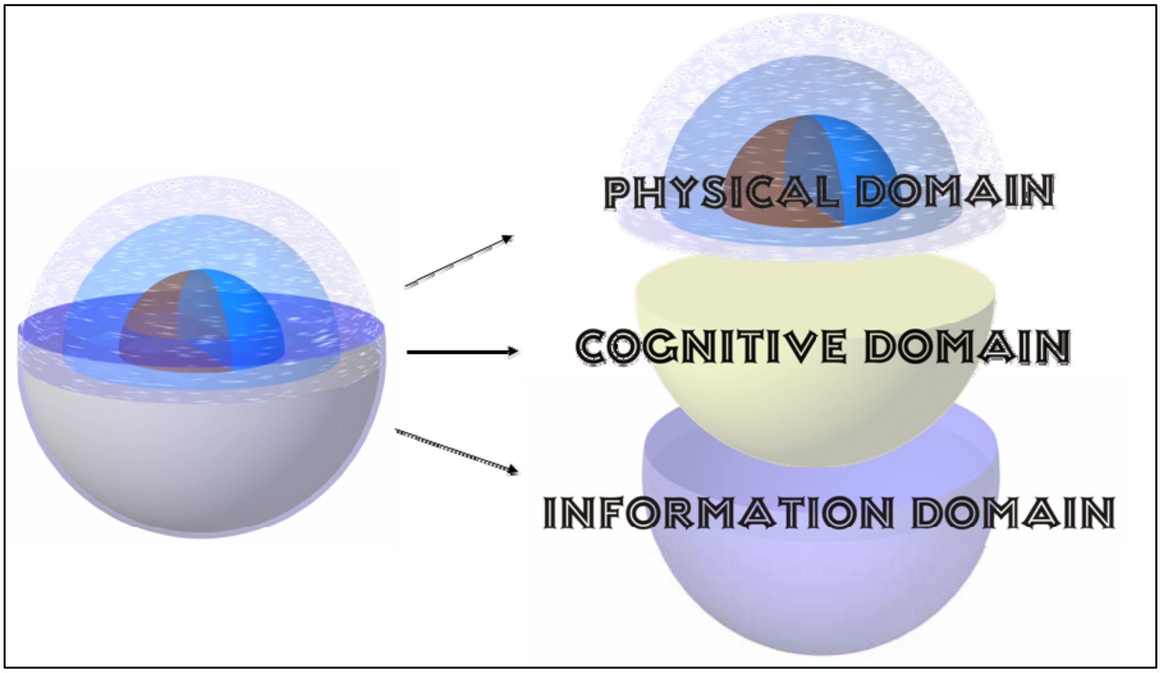


Figure 9 Franz Cyberspace Model [36]

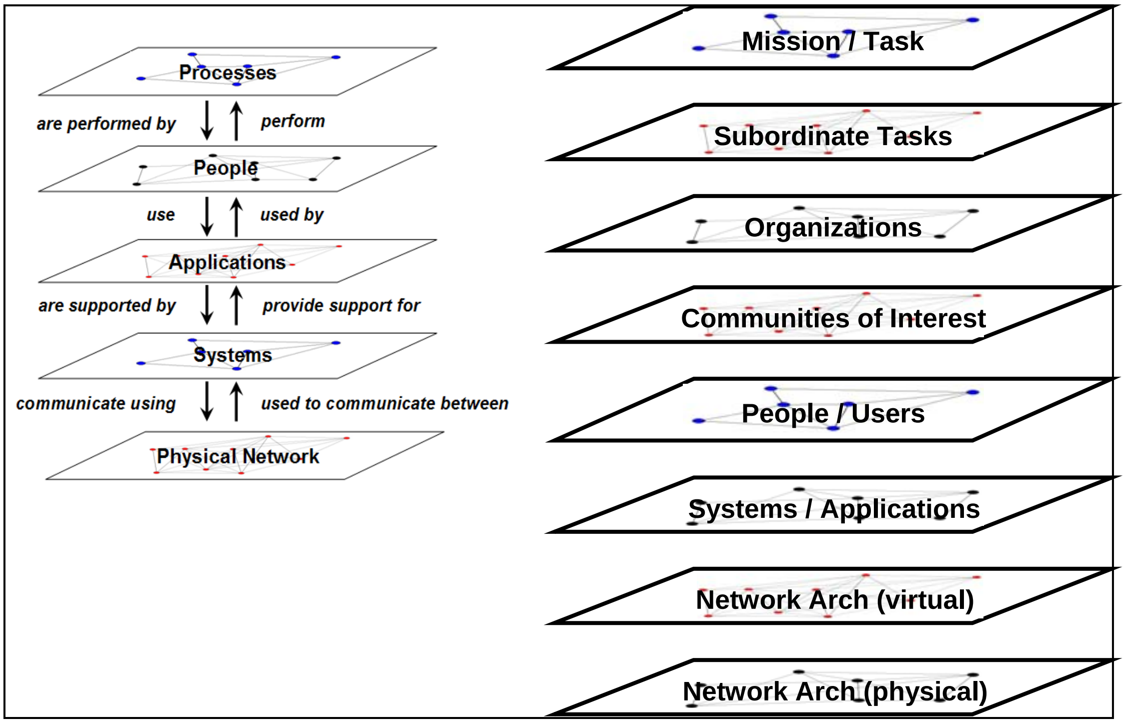


Figure 10 Wong-Jiru and Mills Cyberspace Model [59]

المنارة للاستشارات
www.manaraa.com

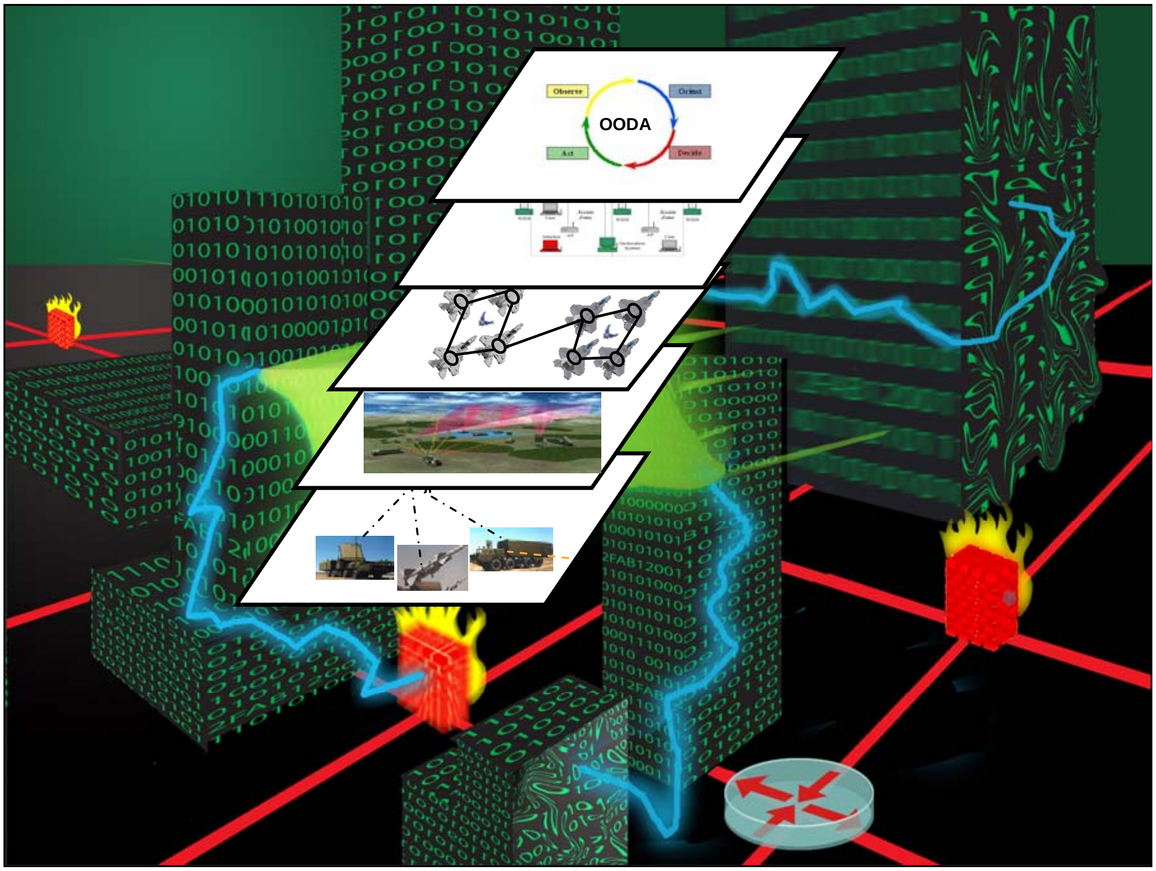


Figure 11 The NCW Battlefield

Putting It All Together

Understand cyberspace and the possibilities it brings to warfighting, comes through integrating these models into the joint planning paradigm. A significant challenge is identifying which agencies within the Air Force can achieve the desired capabilities within cyberspace. Figure 12 depicts the current Air Force Computer Network Operations (CNO) structure. The 315th IOS and the 91st Network Warfare Squadron (NWS) are the primary units responsible for Network Attack (Net-A) in the Air Force.

المنارة للاستشارات
www.manaraa.com

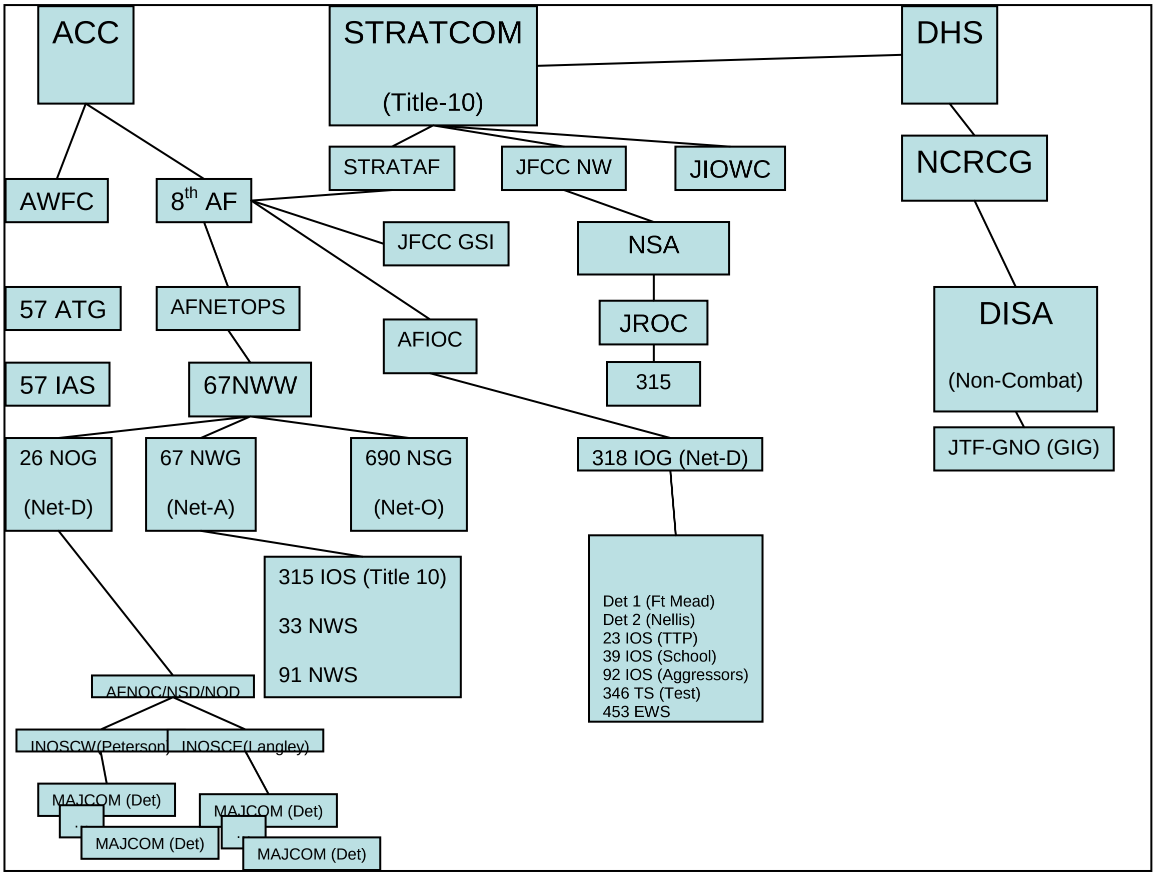


Figure 12 The Air Force CNO Structure

www.manaraa.com

Appendix C – Cyber Flag CONOPS

1.0 Introduction

1.1 Purpose

The Cyber Flag Concept of Operations (CONOPS) outlines the Air Force way ahead for realistic training in air, space, and cyberspace. This CONOPS identifies the requirements necessary to train forces in the air, space and cyberspace domains by leveraging existing capabilities and defining future technologies.

1.2 Background

In April of 1975 the Directorate of Operations, Headquarters Air Force provided a CONOPS briefing for an exercise called Red Flag to attendees of the Fighter Weapons Symposium [15]. The CONOPS detailed Red Flag as a single exercise providing the most realistic training environment possible for aircrews to simulate the first ten combat missions. The idea was that by realistically simulating the first ten combat missions the survival of pilots would markedly improve during actual combat. With the concept approved on 15 July 1975, the first Red Flag began on 27 November 1975 [15].

Using existing assets at either Red Flag-Alaska or Red Flag-Nellis this CONOPS provides a vision for a dedicated exercise intended to emphasize cyberspace capabilities and the way in which they can and will change the face of war fighting.

1.3 Authority

In his 2007 "Letter to Airman" Secretary Michael W. Wynne conveyed the following vision: *"Red Flag exercises, well known as training components of air warfare, will also become a staple of cyber warfare.* [17]" The conflict with existing Red Flag training objectives dictates the creation of a separate venue for the exercise of cyberspace forces in concert with those from air and space.

المنـــارة للاستشارات
www.manaraa.com

1.4 Relationship to other AF CONOPS

This CONOPS supplements the Air Combat Command (ACC) CONOPS for the 57th Adversary Tactics Group (ATG) Aggressors, 10 October 2006.

2.0 Synopsis

2.1 CONOPS

This CONOPS outlines an overarching plan to integrate cyberspace into the operational and tactical levels of Air Force training. More specifically, this document defines a roadmap for establishing a realistic training venue, which encompasses air, space and cyberspace domains. The 57 ATG at Nellis AFB, NV represents "Threats Central" for the USAF [64]. In this capacity, the 57 ATG represents the most fertile ground for the development of the Cyber Flag exercise.

2.2 Objectives

The ACC CONOPS for the 57 ATG states:

> *"In addition, warfighters need to understand their dependence on information systems and communication links and be prepared to operate in information-degraded environments. USAF planners require proper training in an operationally realistic environment that challenges their ability to achieve operational success, while facing a determined and skilled adversary."* [64]

This is achievable to some degree within the existing Red Flag construct but both the competing goals associated with demonstrating effects within cyberspace as well as the sheer breadth of the evolving cyber infrastructure (both in the civilian and military environments) warrant a separate realistic training venue. Cyber Flag provides the overarching objective of demonstrating the critical capabilities of offensive and defensive actions within cyberspace in concert with traditional kinetic operations.

المنارة للاستشارات
www.manaraa.com

2.3 Phased Approach

Because of the fiscal constraints associated with creating a dedicated exercise, three courses of action (COA) provide decision-making options in realizing the overall objective of Cyber Flag.

2.3.1. COA 1: The first option is to extend deployed forces for a one-week period after a Red Flag to support Cyber Flag. The table below provides a sample flow for the week.

Day	M	Tu	W	Th	F
Threat	Thailand	India	Russia	China	China
Level	I	II	III	III	III
Types	C2	C2 & SCADA	C2 & SCADA	C2&Airborne	All
Vulnerability	Patches	Patches & Protocol	Patches & Protocol	Phishing, Virus Worm	All
Effect	Scans (IPB)	Scans & Hooks	Web Page Deface, Anomalous Activity	Data Extraction, DOS, EA	All

The threat levels provide a graduated learning environment where:

Level I: Benign Targets

Level II: Defended Targets

Level III: Aggressive Target (i.e. shoots back)

These threats and target types represent the current focus for operational planning and tactical employment during the week of Cyber Flag. The networks supporting the operational planning would be subject to the effects listed above given the type of vulnerabilities that exist. The CAOC would be under constant attack and ATO production must continue to fuel the tactical missions. If it is impractical to have the

المنارة للاستشارات
www.manaraa.com

Nellis CAOC attacked, then a notional CAOC, tied to the Joint IO range, could produce products in parallel with those used to fly actual missions. Mission planning would ensure target pairing to both kinetic and non-kinetic capabilities.

Pros: This option would preserve existing Red Flag training objectives accomplished during the previous week's missions. The cyberspace domain would be the emphasis of the additional week of training. This is an optimal scenario because it allows a robust Air Expeditionary Force to employ together against the most realistic threat while focusing on the enabling effects within cyberspace.

Cons: Funding for unit deployments would have to be increased but costs compared to deploying and redeploying the necessary forces are minimal.

2.3.2. COA 2: Another option is to create a network infrastructure like Bulwark Defender with nodes at Air Force Bases that have aircraft. The table below provides a suggested force structure with associated participants.

Squadron	Role	Base
1st Fighter Wing (F-15 / F-22)	Offensive Counter Air / Red Air	Langley AFB, VA
ACC NOSC / INOSC	Command and Control	Langley AFB, VA
2nd Bomb Wing (B-52)	Interdiction / Strike	Barksdale AFB, LA
AFNOC	Command and Control	Barksdale AFB, LA
8th AF	CAOC	Barksdale AFB, LA
33 IOS	Net-D	Lackland AFB, TX
315 IOS	Net-A	Ft George Mead, MD
355th Wing (A-10)	CAOC / CAS	David Monthan, AZ
SOCOM	CAOC	Hurlburt AFB, FL
57 IAS	Information Aggressors	Nellis AFB, NV

Aggressors would conduct network warfare against the operational command elements of the network while Blue Forces task aircraft to provide tactical support. In

www.manaraa.com

addition, aggressors would implement elements of CNA, CND, PSYOPS and EW at the tactical level by targeting base-level communications infrastructure.

Pros: This would be the lowest cost option for Cyber Flag because bases could support the exercise without the deployment of aircraft. The aircraft could also fly alternate missions if the cyber effects prevented them from executing the primary tasking. A base-level exercise would also exhibit a broad range of cyber effects to a very diverse audience including communications, maintenance, aviation, and security police personnel. Jamming could take place against cell phones and land mobile radios. Internet attacks could start with propaganda via web pages and phishing attacks aimed at gaining network access. The escalation of the exercise could then see complete denial of service attacks against networks on base similar to an "Alarm Black" type event during a Phase II.

Cons: This would require base-level participation similar to a Phase II exercise. Nearly all base operations would necessarily cease except those supporting the exercise.

2.3.3 COA 3: The final option is to deploy forces for a dedicated Cyber Flag exercise in which the objectives support effects based primarily on non-kinetic means.

Pros: There is nothing better than a dedicated venue for highlighting the enabling capabilities of cyberspace.

Cons: The lack of money available to spend on additional training or to upgrade existing training is a growing concern. There will have to be a tremendous reprioritization of funding for training and programs to enable this type of Cyber Flag.

المنارة للاستشارات
www.manaraa.com

3.0 Time Horizon, Assumptions and Risks

3.1 Time Horizon

A Cyber Flag exercise utilizing COA 1 is feasible within the current or next Fiscal Year, if funding for additional exercise days exists. Based on existing Red Flag and Air Expeditionary Force flows, COA 2 and 3 allow implementation within Fiscal Year (FY) 09 at the earliest.

3.2 Assumptions

This document assumes the existing timeline for FY 11 ATG end strength.

3.3 Risks

As ACC CONOPS for the 57 ATG states:

> *"Threat identification and focus will be inherent risks of this program. The Aggressors must strike a balance between accurately replicating the range of threats AF forces may encounter and risking a dilution of their efforts, by trying to train themselves and their audience for too many things and none well."* [64]

4.0 The Overall Military Challenge

4.1 General

The continued downsizing of the Air Force means fewer resources (people and money) to support an increasing number of requirements. The addition of a new exercise requires a significant amount of funding. As a result, there must be an analytical effort to define the true funding priorities given the potential threat. The threats within cyberspace present significant challenges to both the US, in general, and the USAF, in particular, requiring a proportionate level of emphasis on training.

المنارة للاستشارات
www.manaraa.com

4.2 Description

The 57th ATG relies on the 57th Information Aggressor Squadron (IAS) to provide a representative cyberspace threat to Red Flag participants. To realize this objective, however, information aggressors jeopardize aircrew-training requirements.

5.0 Desired Operational Effects

5.1 End-state

The overall effect of Cyber Flag is to create a realization across the Air Force regarding the importance of cyberspace capabilities and to provide in-depth training to meet the rapidly and ever-increasing cyber threat on a national and military basis.

5.2 Desired Effects

This venue provides USAF and Joint training against a realistic threat presented through air, space and cyberspace leading to the development of blue tactics, techniques and procedures.

6.0 Necessary Capabilities

The Joint Information Operations (IO) Range and a suitable conventional range, such as the Nevada Test and Training Range (NTTR), are necessary for Cyber Flag.

7.0 Enabling Capabilities

The capability to replicate red and blue network environments on the Joint IO Range is necessary to present a realistic cyberspace-training environment. The Virtualized Intranet Platform for Exercise Realism (VIPER) provides this capability using the Lincoln Adaptable Real-time Information Assurance Testbed (LARIAT).

المنارة للاستشارات
www.manaraa.com

8.0 Command Relationships / Architecture

The existing command structure of the 57 ATG is preserved under this CONOPS with the administration of the Cyber Flag exercise falling under the 57 Adversary Tactics Support Squadron, the 414 Combat Training Squadron (Red Flag), and the 57 IAS.

9.0 Summary

In accordance with the CSAF vision for the 57 ATG, this CONOPS provides a robust threat environment to enhance training in air, space and cyberspace.

المنارة للاستشارات
www.manaraa.com

Bibliography

1. Christian Lowe, “Air Force, Cyberspace Defenders” http://www.defensetech.org/archives/002007.html

2. Joint Forces Command, *Major Combat Operations Joint Operating Concept*, December 2006, http://www.dtic.mil/futurejointwarfare/concepts/mco_joc_v20.doc.

3. Secretary Michael W. Wynne, *Letter to Airman*, 7 May 2007, http://www.af.mil/library/viewpoints/secaf.asp?id=320

4. Charles F. Shaver, *Irregular Warfare Special Study*, 4 August 2006, http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA455415

5. Joint Chiefs of Staff, *Joint Net-Centric Operations Campaign Plan,* October 2006, 62, http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf

6. Tom Espiner, *Security Experts Lift Lid on Chinese Hack Attacks,* 2007, http://news.zdnet.com/2100-1009_22-5969516.html

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

8. Michael Skinner, *Red Flag: Air Combat for the ‘80s,* (Novato, CA: Presidio Press, 1984).

9. AFDD 2-1, *Air Warfare*, 22 January 2000.

10. Nathan D. Broshear, “First Virtual Flag of 2006 Ends” (ACC) http://www.acc.af.mil/news/story.asp?id=123013726

11. “BD06 Confirms Joint CND Capability” Spokesman Magazine, April 2006, http://findarticles.com/p/articles/mi_m0QUY/is_4_46/ai_n16135398.

12. Department of Defense, RDT&E Budget Item Justification (Washington, DC) http://www.dtic.mil/descriptivesum/Y2008/OSD/0303166D8Z.pdf.

13. A. Murphy, “Crash Testing the TIF” (January 2007) http://public.afca.af.mil/news/story.asp?id=123039553 (accessed 17 Apr 07).

للاستشارات المنارة
www.manaraa.com

14. Timothy L. Thomas, *Dragon Bytes; Chinese Information-War Theory and Practice*, (Ft Leavenworth, KA: Foreign Military Studies Office, 2004).

15. Major Alexander Berger, “Beyond Blue Four,” Air & Space Power Journal (Summer 2005), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/sum05/berger.html

16. Sam Arwood, “Cyberspace as a Theater of Conflict: Federal Law, National Strategy and the Departments of Defense and Homeland Security,” (Graduate Research Project Wright-Patterson AFB, OH: AFIT, 2007).

17. Secretary Michael W. Wynne, “Flying and Fighting in Cyberspace,” Air & Space Power Journal, (Spring 2007), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/spr07/wynnespr07.html.

18. General T. Michael Moseley, “CSAF’s Vector: Advanced Composite Force Training,” (5 Jan 2006), http://www.af.mil/library/viewpoints/csaf.asp?id=207.

19. Paul Jackson, *Jane’s All The World’s Aircraft 2005-2006* (UK: Jane’s Information Group, 2005)

20. General Wilbur L. Creech, interview by Hugh Ahmann, June 1992, transcript, 192, AFHRA, K239.0512-2050.

21. Benjamin S. Lambeth, The Transformation of American AirPower (Ithaca, NY: Cornell University Press, 2000).

22. Paul Huffman, “Aggressor Transformation: Beyond The Flightline” (Maxwell AFB, AL: Air War College, 2006).

23. T. Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?* (Fort Leavenworth, KS: US Army War College, 2001), pp. 6-7, 19, 21.

24. K. Gauthier, “*China as Peer Competitor?” (*Maxwell AFB, AL: Air War College, 1999), p. 20.

25. J. Mulvenon and R. Yang, *The People’s Liberation Army in the Information Age.* (RAND, 1999), pp. 182-183.

المنارة للاستشارات
www.manaraa.com

26. Wang Pufeng (2000). *The Challenge of Information Warfare*, p. 2. Retrieved 1 Jul 06 from, www.fas.org.

27. Timothy L. Thomas, *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice*. (Fort Leavenworth, KS: Foreign Military Studies Office, 2001), pp. 10-18.

28. Baocun and Fei. (1996). *Information Warfare*, p. 2. Retrieved 4 Aug 06 from, http://www.fas.org/irp/world/china/docs/iw_wang.htm.

29. *China's Defense Budget*. Retrieved 4 Jul 06 from www.globalsecurity.org.

30. *China's Military Spending May be Higher Than Acknowledged*. Retrieved 4 Jul 06 from www.defensenews.com.

31. *China's Defense Budget*. Retrieved 4 Jul 06 from www.globalsecurity.org.

32. Department of Defense (Jan 03). *Joint Tactics, Techniques and Procedures for Intelligence Support to Targeting; Joint Pub 2-01.1*. Joint Staff, pp. 1-50.

33. Joint Forces Staff College (Jul 03). *Joint Information Operations Planning Handbook*. National Defense University, pp. 1-56.

34. Department of Defense (Feb 98). *USAF Intelligence Targeting Guide: Air Force Pamphlet 14-210*. United States Air Force, pp. 1-135. Retrieved 10 Aug 06, from, http://www.fas.org/irp/doddir/usaf/afpam14-210/part06.htm.

35. Fayette, D. (Jun 01). *Effects-Based Operations*. Air Force Research Laboratory, p. 1. Retrieved 30 Aug 06 from, http://www.afrlhorizons.com/Briefs/Jone01/IF00015.html.

36. Timothy P. Franz, *IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-ahead for Network Warfare Forces*. (Masters Thesis Wright-Patterson AFB, OH: AFIT, 2007).

37. Maj Timothy P. Franz, Maj Matthew F. Durkin, Maj Paul D. Williams, Maj Richard A. Raines (Ret), LtCol Robert F. Mills (Ret) "Defining Information Operations Forces: What Do We Need?" Air & Space Power Journal, (Summer 2007).

38. LtCol David T. Fahrenkrug, "Cyberspace Defined," *The Wright Stuff*, 17 May 07.

39. G. Zimmerman. "The United States Air Force and Cyberspace: Ultimate Warfighting Domain and the USAF's Destiny," (Washington, DC: Cyberspace Task Force, 2006).

المنارة للاستشارات
www.manaraa.com

40. Mark Kanko. “Information Operation Range Visualization Requirements.” (White Paper Lackland AFB, TX: BAH, 2006).

41. Lt Col Rob Spalding, “Why Red Flag Is Obsolete,” *Air & Space Power Journal* (Fall 2006), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj06/fal06/spalding.html.

42. Nathan Thornburgh, “Inside the Chinese Hack Attack,” *TIME*, 25 Aug 05, http://www.time.com/time/nation/article/0,8599,1098371,00.html.

43. Jeanne Meserve, “Staged Cyber Attack Reveals Vulnerability in Power Grid,” *CNN*, 26 Sep 07, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html.

44. Michael R. Gordon, “U.S. Command Shortens Life of ‘Long War’ as a Reference,” *The New York Times*, 24 Apr 07, http://www.nytimes.com/2007/04/24/washington/24policy.html.

45. Erik Holmes, “Lord to Oversee Cyber Command,” *Air Force Times*, 26 Sep 07, http://www.airforcetimes.com/news/2007/09/airforce_cyberboss_070924w/

46. Tamara Yu, Benjamin Fuller, John Bannick, Lee Rossey, Robert Cunningham “Integrated Environment Management for Information Operations Testbeds,” 29 Oct 07, [online], http://www.vizsec.org/workshop2007/presentations/yu-testbed.pdf.

47. Ian Urbina “Psy-Ops: The Fine Art Of War Propaganda,” *Monitor*, 23 December 2002, http://www.albionmonitor.com/0212a/psyops.html.

48. “BD06 Confirms Joint CND Capability,” *Spokesman Magazine*, April 2006, http://findarticles.com/p/articles/mi_m0QUY/is_4_46/ai_n16135398.

49. Master Sgt. Tonya Keebaugh and Senior Airman Travis Edwards, “Air Warrior transforms into new Green Flag,” *Air Force Link*, 4 Oct 06, http://www.af.mil/news/story.asp?storyID=123028387.

50. Captain Thomas J. Norton, “Blue Flag,” *Air University Review*, 11 Jul 02, http://www.airpower.maxwell.af.mil/airchronicles/aureview/1979/jan-feb/norton.html.

51. 1st Lt Nathan D. Broshear, “First Virtual Flag exercise of 2006 ends,” *Air Combat Command News*, 14 Nov 05, http://www.acc.af.mil/news/story.asp?id=123013726.

52. Kenya Shiloh, “AFIWC concludes Black Demon exercise,” *Spokesman Magazine*, April 2005, http://findarticles.com/p/articles/mi_m0QUY/is_2005_April/ai_n15342557.

53. Aaron Hansen, “BD06 confirms joint CND capability,” Spokesman Magazine, April 2006, http://findarticles.com/p/articles/mi_m0QUY/is_4_46/ai_n16135398.

المنارة للاستشارات
www.manaraa.com

54. Henry S. Kenyon, “Air Force Aims for rapid Deployment And Continuous Operational Awareness,” *SIGNAL*, Nov 99, http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=800&zoneid=140.

55. Admiral Walter F. Doran, “Pacific Fleet Focuses on War Fighting,” *Proceedings*, August 2003, http://www.pacom.mil/news/news2003/0308JTF519.pdf.

56. “Maple Flag,” http://www.airforce.forces.gc.ca/4wing/training/mapleflag/about_e.asp.

57. “Northern Edge History,” *Elmendorf Air Force Base Fact Sheet*, http://www.elmendorf.af.mil/library/factsheets/factsheet.asp?id=5380.

58. Pamela L. Woolley, “Defining Cyberspace as a United States Air Force Mission,” (Masters Thesis Wright-Patterson AFB, OH: AFIT, 2006).

59. Ann Wong-Jiru and Mills, “Graph Theoretical Analysis of Network Centric Operations Using Multi-Layer Models,” (Masters Thesis Wright-Patterson AFB, OH: AFIT, 2006).

60. Jim DeBrosse, “Dayton’s first-ever international hackers convention gets under way on Saturday,” *Dayton Daily News*, 9 Oct 07, http://www.daytondailynews.com/n/content/oh/story/news/local/2007/10/08/ddn100907hackers.html.

61. Ian Traynor, “Russia accused of unleashing cyberwar to disable Estonia,” *The Guardian*, 17 May 07, http://www.guardian.co.uk/russia/article/0,,2081438,00.html.

62. William A. Sayers, “The Red Baron reports what they really said,” *Airpower History*, 22 Sep 05, http://goliath.ecnext.com/coms2/browse_R_A106.

63. Roger C. Molander, Peter A. Wilson, B. David Mussington, Richard Mesic “Strategic Information Warfare Rising,” *RAND*, 1998.

64. “Concept of Operations for the 57th Adversary Tactics Group,” *Air Combat Command*, 10 Oct 06.

المنارة للاستشارات

www.manaraa.com

65. Rossey, L., Cunningham, R., Fried, D., Rabek, J., Lipmann, R., Haines, J., Zissman, M. (2002) "LARIAT: Lincoln Adaptable Real-time Information Assurance Testbed", IEEE, Aerospace Conference Proceedings, Vol. 6, pp 2671-2678.

66. Steve Coll and Susan B. Glasser "Terrorists Turn to the Web as Base of Operations," *Washington Post*, 7 Aug 05, A01.

67. George Hulme "The Mind of a Hacker," *Information Week*, 10 Nov 03, http://www.informationweek.com/story/showArticle.jhtml?articleID=16000606.

68. Mark Landler and John Markoff "Digital Fears Emerge After Data Siege in Estonia," New York Times, 29 May 07, http://www.nytimes.com/2007/05/29/technology/29estonia.html.

69. Robert K. Yin, *Case Study Research: Design and Methods*, (Thousand Oaks, CA: Sage Publications, 2003).

70. Nathan D. Broshear "Blue Flag starts with a bang at Nellis, Hurlburt Field," Air Force Link, 25 Jul 05, http://www.af.mil/news/story.asp?storyID=123011117.

71. Raid Qusti "Experts Recommend Special Laws to Combat Terror," *Arab News*, 5 Dec 07, http://www.arabnews.com/?page=1&section=0&article=104300&d=5&m=12&y=2007&pix=kingdom.jpg&category=Kingdom.

72. "Rise In International Cyber Spying Will Pose Biggest Security Threat In 2008," *Security Products*, 3 Dec 07, http://www.secprodonline.com/articles/56400/.

73. Fotinger, C and Ziegler, W., *Understanding a Hacker's Mind – A psychological insight into the hijacking of identities*, (Danube-University Krems, Australia, 2004).

74. Raymond, E., "How to become a hacker," 23 Apr 04, http://www.catb.org/~esr/fags/hacker-howto.html.

75. Bill Gertz, "Hackers linked to China stole Los Alamos documents," The Washinton Times, 3 Aug 00, http://www.rpatrick.com/tech/malware/china/.

76. John E. Dunn, "Hackers Launch Major Attack on US Military Labs," *PC World*, 7 Dec 07, http://www.pcworld.com/article/id,140390-c,hackers/article.html.

المنارة للاستشارات

www.manaraa.com

77. 414 Combat Training Squadron Mission Statement, *57th Wing Fact Sheet*, Nellis AFB, NV, [online], http://www.nellis.af.mil/library/factsheets/factsheet.asp?id=4098.

المنارة للاستشارات

www.manaraa.com

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 27-03-2008	**2. REPORT TYPE** **Master's Thesis**	**3. DATES COVERED** *(From – To)* Jun 2006 – Mar 2008

4. TITLE AND SUBTITLE Cyber Flag: A Realistic Cyberspace Training Construct	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Hansen, Andrew P., Major, USAF	**5d. PROJECT NUMBER** ENR #07-122
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Electrical and Computer Engineering (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GCS/ENG/08-10
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFRL/RHX Attn: Capt Larry W. Fortson 2255 H Street, Bldg 248 WPAFB OH 45433-7022 DSN: 674-5737 Email: Larry.Fortson@wpafb.af.mil	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

As is well understood, the rapidly unfolding challenges of cyberspace is a fundamental warfare paradigm shift revolutionizing the way future wars will be fought and won. A significant test for the Air Force (indeed any organization with a credible presence in cyberspace) will be providing a realistic training environment that fully meets this challenge. Why create another Flag level exercise? Realistic training (that which is effective, comprehensive and coordinated) is crucial to success in time of war. Red Flag provides dominant training within the air domain and now with the evolution of cyberspace, a comprehensive training environment is necessary to meet this growing and broadening threat. This Thesis builds on the Red Flag tactical training exercise in order to define a future environment that combines the air, space and cyberspace domains with specific emphasis on cyberspace capabilities and threats. Red Flag has and continues to be a great tactical training exercise; Cyber Flag would use the best practices of Red Flag (and other realistic training venues) to define a future training environment for the cyberspace domain. There is no better training than the hands-on realism associated with participation in an exercise such as Red Flag. Secretary Michael W. Wynne has a vision for dominant operations in cyberspace "comparable to the Air Force's global, strategic omnipresence in air and space." This bold vision requires a combination of joint coordination, skilled forces and a realistic training environment to bring them all together; Cyber Flag is the suggested vehicle for accomplishing this.

15. SUBJECT TERMS
Cyberspace, Training, Red Flag

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Paul D. Williams, Maj, USAF (ENG)
REPORT **U**	**ABSTRACT** **U**	**c. THIS PAGE** **U**	**UU**	134	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636 x7253; e-mail: Paul.Williams@afit.edu

www.manaraa.com