COMMERCIAL AIR CARRIER VULNERABILITIES TO INFORMATION OPERATIONS

GRADUATE RESEARCH PROJECT

Bryan H. Shelburn, Major, USAF

AFIT/GMO/ENS/02E-11

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GMO/ENS/02E-11

COMMERCIAL AIR CARRIER VULNERABILITIES TO INFORMATION OPERATIONS

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Operational Sciences

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 Air Mobility

Bryan H. Shelburn, B.S.

Major, USAF

6 June 2002

Acknowledgements

First I would like to thank my advisor, Dr. Richard Deckro, for his helpful insight into the subject matter of this paper, and for putting me in touch with so many valuable sources of information. One of these sources that I also would like to thank is Mr. Marty Henry, Air Force Representative to the Joint Program Office for Special Technologies Countermeasures in Dahlgren Virginia, whose knowledge of critical infrastructure protection was very helpful. Next I would like to thank General (Retired) Walter Kross of Flight Explorer and Mr. Charles Beard of KPMG Consulting for their commercial industry perspective on the subject of information warfare. In addition, I would certainly like to thank Ms. Janice Missildine whose assistance in procuring research material was absolutely essential to completing this paper. Finally, I would like to thank my wife, whose encouragement and support were just what I needed to further my education and professional development.

Table of Contents

Acknowledgements iii
Table of Contents iv
List of Figures v
List of Tables v
Abstract vi
I. Introduction 1
Background 1
Research Question 4
Scope 5
Assumptions and Stipulations 5
Outline of Remaining Chapters 5
II. Literature Review 6
Department of Defense/Joint Publications 6
Joint Vision 2020 6
Joint Pub 3-13 Joint Doctrine for Information Operations 7
Service Doctrines 10
U.S. Army 10
U.S. Air Force 12
U.S. Marine Corps 16
Government Reports 17
Government Accounting Office (GAO) Reports 18
Congressional Testimony 21
Commercial Perspectives on Information Assurance Research 23
Journal Publications/Periodicals/Other Published Research 24
Interviews with Experts 28
III. Methodology 32
Operational Dependency Matrix 32
Analyzing Contract Airlift 34
Risk Assessment 39
Summary 41
IV. Conclusions and Discussion 42
References 44

List of Figures

Figure 1. CERT Incidents Reported 4
Figure 2. Information Environment Protection 9
Figure 3. U.S. Army Depiction of Information Operations 10
Figure 4. Evolution of Data to Understanding 12
Figure 5. Air Force Doctrine Depiction of Information Operations 13
Figure 6. Operational Dependency Matrix 33
Figure 7. Information Flow for AMC Operations at BWI 38
Figure 8. Risk Management Framework 39
Figure 9. Risk Management and the Value of Information Model 40

List of Tables

Table 1. Categories of System Vulnerabilities 25

Abstract

The conduct of Information Operations by the United States Military and its enemies is changing because of the rapid development of information technology. The increasing dependence of government and industry on information technology has created critical vulnerabilities that can be exploited by degrading or destroying the use of information systems. Among those elements susceptible to these vulnerabilities are the operations of commercial air carriers that are essential to the military's ability to wage war and project power wherever needed in the world. These threats must be seriously examined and mitigated to ensure that commercial air carriers can fulfill their roles in our national security strategy.

This study reveals potential Information Operations vulnerabilities in the commercial air carriers' conduct of missions for the military. The systems used by Air Mobility Command to plan and track the operation of contracted airlift, and those used by the airlines to operate their flight schedule, are susceptible to physical and cyber attacks. A potential result of a successful attack is a dramatic slowdown in the operation of commercial air carriers that could lead to unacceptable delays in transporting combat forces where they are needed to execute national military objectives.

I. Introduction

> "… let us go down, and there confound their language, that they may not understand one another's speech."
>
> Genesis 11:7

Background

According to the Bible, God was able to stop the construction of the Tower of Babel by destroying the ability of people to communicate with one another. Likewise, most organizational units (families, businesses, governments, armies) rely on their ability to communicate information between various segments of the organization to be successful. Destroying or disrupting the information or information systems can render the organization dysfunctional.

Everything changes; warfare is no exception. The events of 11 September 2001 showed that the United States, with the most powerful and best-equipped military in the world, is still vulnerable, even to enemies with far less sophisticated weaponry, tactics, and training. The conduct of asymmetrical warfare exploits dependencies and vulnerabilities in systems relied on by the powerful to the advantage of the less powerful. Usually considered strategically ineffective (short term damage easily overcome), asymmetric threats to the United States are continually expanding. This is especially true in the area of information operations. Information technology's critical role in national security, coupled with the relatively low level of effort required to exploit it, has made protecting information technology (IT) infrastructure and systems from attack a whole new chapter in national military strategy. All units in the Department of Defense, as well as their contractors and suppliers, must continually assess their vulnerabilities to an

adversary's information operations to be effective in their role in fighting and supporting America's wars. Vigilance has become everyone's duty and responsibility in today's environment.

In order to successfully fight wars, the military must maintain a flexible, responsive transportation system capable of delivering forces, with their equipment, to the battlefield and sustain them as needed. Recent reductions in forces, coupled with lean logistics initiatives, have made this capability more critical than ever. In the post Cold War environment, the U.S. has chosen to drastically reduce the number of troops and equipment pre-positioned overseas. In addition, since the collapse of the former Soviet Union, formulating national military strategy has been far more challenging because the major threats to the U.S.'s national security are far less predictable. Pre-positioning forces becomes less desirable because of the need to be flexible; if we cannot know in advance where we are to fight, we should train at home and be prepared to deploy to where the fight happens. In addition, it may be easier and more desirable to provide force security at home rather than abroad. This requires rapid global mobility in order to deploy the appropriate forces wherever they are needed in the world to conduct operations. In the words of Dr. William Cunningham, a professor at the Air Force Institute of Technology lecturing on the strategic mobility of combat forces, the U.S. has decided to "trade inventory for transportation."

The United States Transportation Command (USTRANSCOM or USTC) is charged with overseeing the transportation mission of all the armed forces. In addition to managing those "organic" transportation assets owned by all the armed services, USTRANSCOM arranges for contracting commercial carriers (trucks, railroads, airlines

and, commercial ships) to provide the military with transportation, since the military's organic lift capacity is insufficient for large scale deployments. These commercial partners' contributions to national defense are vital to any major regional conflict. According to draft testimony approved by the Commander in Chief (CINC) of USTRANSCOM and scheduled to be delivered by TRANSCOM's J-2 (director of intelligence) in June 2002 to the House Select Committee on Intelligence, "80 % of everything USTRANSCOM moves in support of DoD moves through commercial carriers." 80% of all passengers transported by Air Mobility Command (AMC) in fiscal year 2000 traveled on a commercial aircraft (USTRANSCOM TCJ4-BC, 2001:80). While the ability to move troops and cargo using commercial carriers greatly enhances the military capabilities of the U.S., this practice makes these commercial carriers not just targets for terrorism, but strategic, high-value targets for the enemies of the United States.

Technology has driven both government and industry to be increasingly reliant on the Internet for rapid and efficient processing of information. According to the same upcoming testimony by TRANSCOM J-2, 70% of all DoD NIPRNET (Non-Secure Internet Protocol Router Network) traffic is carried on the Internet at some point between sender and receiver. Empirical statistical evidence is growing to reveal the severity of cyber security threats. Figure 1 shows the exponential increase in incidents handled by the Computer Emergency Response Team (CERT®). The chart shows that the number of incidents detected *and reported* has more than doubled each year since 1998 (Hamill et al., 2002).

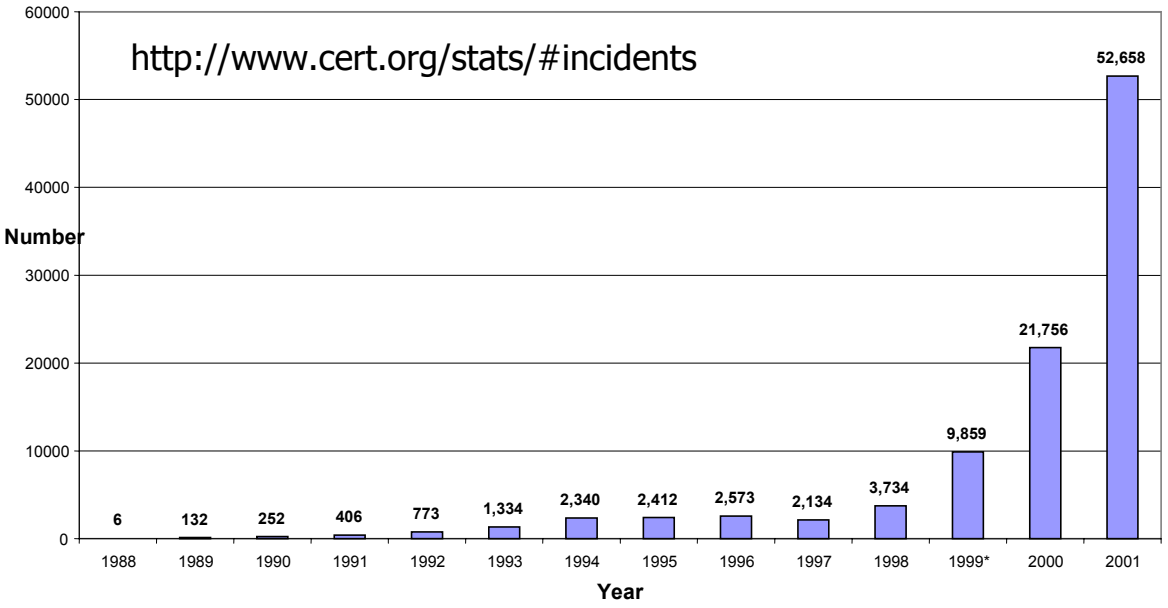

Figure 1. CERT Incidents Reported (Hamill et al., 2002)

According to the Computer Security Institute's 2000 Computer Crime and Security Survey, which analyzed 643 responses from corporations and government agencies, financial losses from computer crime increased from $100 million in 1997 to over $265 million in 2000 (Fisher:2001). While fiscal issues are critical to our economic well being, the military must be prepared to deal with the national security aspects of conducting so much business with commercial partners and simultaneously relying on technology that can be exploited by its enemies.

Research Question

This study focuses on two key issues at the unclassified level. When using these commercial carriers to aid in the conduct of military operations, what are the potential information operations vulnerabilities that must be planned for? What elements of the

nation's critical infrastructure are essential to enabling commercial airlines to operate and how might an adversary attack them with asymmetric warfare?

Scope

Due to the vast scale of USTC's commercial airlift operations, this research will focus of on a limited segment of USTRANSCOM's commercial airlift operations. The intent is to give operations planners a framework for analyzing other segments (different airports, carriers and subcontractors) in order to assess the vulnerabilities of total network of transportation providers. This study will be limited to analyzing and reporting information at the unclassified level.

Assumptions and Stipulations

More is known about the vulnerabilities of Information Operations than can be studied or revealed in this paper due to classification levels and the need to protect that information from potential adversaries.

Outline of Remaining Chapters

Chapter II will present a review of current literature on the study of asymmetric warfare, critical infrastructure protection and information operations. Chapter III will present a methodology for assessing Information Operations (IO) vulnerabilities. Chapter IV will present conclusions and recommendations from this study.

II. Literature Review

One certainty in reviewing the current literature about modern information operations (IO) is that very little consensus exists on how to best conduct IO. The emergence of information warfare in our time could reasonably be compared to the advent of air power in the early 20th century—most experts agreed that the use of air assets would forever change the conduct of warfare. Developing consistent, reliable doctrine and tactics, however, remains an enormous and constantly changing challenge.

Department of Defense/Joint Publications

Joint Vision 2020

The Chairman of the Joint Chiefs of Staff (CJCS), in addition to his statutory responsibility for forming the national military strategy, published Joint Vision 2020 as "a template to guide the continuing transformation of America's armed forces (JV 2020, 2000:1)." Though not meant to prescribe or describe specific weapon systems or combat tactics, this document attempts to describe the future military operating environment and the warfighting capabilities needed for success in maintaining the security of the United States. It is significant to note that one of the CJCS's six operational concepts—meant to guide strategic thought by current and future military leaders—is information superiority. JV 2020 recognizes the ability of information technology to provide adversaries increased capabilities creates the need to aggressively prepare for these asymmetric tactics. Though many fundamentals of warfare will never change (no level of IT will eliminate the inevitable fog of war, which may actually be made worse by an IO attack)

asymmetric capabilities are significantly changing the conduct of warfare now and in the future.

Information superiority, as defined by JV 2020 is "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (JV 2020, 2000:10)." Achieving information superiority serves no purpose by itself; the attainment of information superiority must be translated into superior knowledge and decisions (JV 2020, 2000: 11).

Joint Pub 3-13 Joint Doctrine for Information Operations

JP 3-13 is intended to serve four main functions for Joint Force Commanders:

1. Define the objectives of information operations.
2. Address the details of offensive and defensive information operations.
3. Give guidance concerning information operations planning.
4. Discuss organizational and training issues.

Simply stated, information operations are actions taken to affect adversary information and information systems while defending one's own information and information systems (JP 3-13, 1998:vii). They are conducted at all three levels of warfare (strategic, operational and tactical). At the strategic level, the President and the Secretary of Defense conduct IO to affect an enemy's broad national power while defending the United States from similar actions. At the operational level, theater commanders conduct IO to achieve campaign objectives and are often focused on the adversary lines of communications. At the tactical level, unit commanders conduct IO to achieve victory in battle (JP 3-13, 1998:I-2).

At all levels, IO's focus is on the vulnerabilities and opportunities created by the increasing reliance on information technology to affect the decision maker. One significant aspect of the Joint Doctrine is that there is very little differentiation between information operations and information warfare, as compared with Air Force Doctrine (to be discussed later). According to JP 3-13, information warfare is simply IO conducted during wartime.

Specifics that relate to the topic of this study can be found in Chapter 3, Defensive Information Operations, of JP 3-13. While primarily focused on protecting the information and information systems under the control of the armed services, parallels can, and must be, made in order to protect the critical assets and infrastructures used by commercial air carriers conducting missions for the Department of Defense. JP 3-13 discusses the integration of activities of other government agencies into the Joint Force Commander's operation, but does not directly discuss integrating the DoD's activities into assuring those activities will be viable when needed. The major elements of successful defensive information operations are:

1. Information Assurance
2. Information Security
3. Physical Security
4. Operations Security
5. Counter-deception
6. Counter-propaganda
7. Counter Intelligence
8. Electronic Warfare
9. Special Information Operations

(JP 3-13, 1998:III-1)

The focus of defensive IO is to create a "protected information environment." Joint Force Commanders accomplish this by first determining the value of the information they control. From there, they employ policies, procedures, protective

technologies, and operations to create the desired environment (JP 3-13, 1998: III-8). See Figure 2 for a depiction of this process.

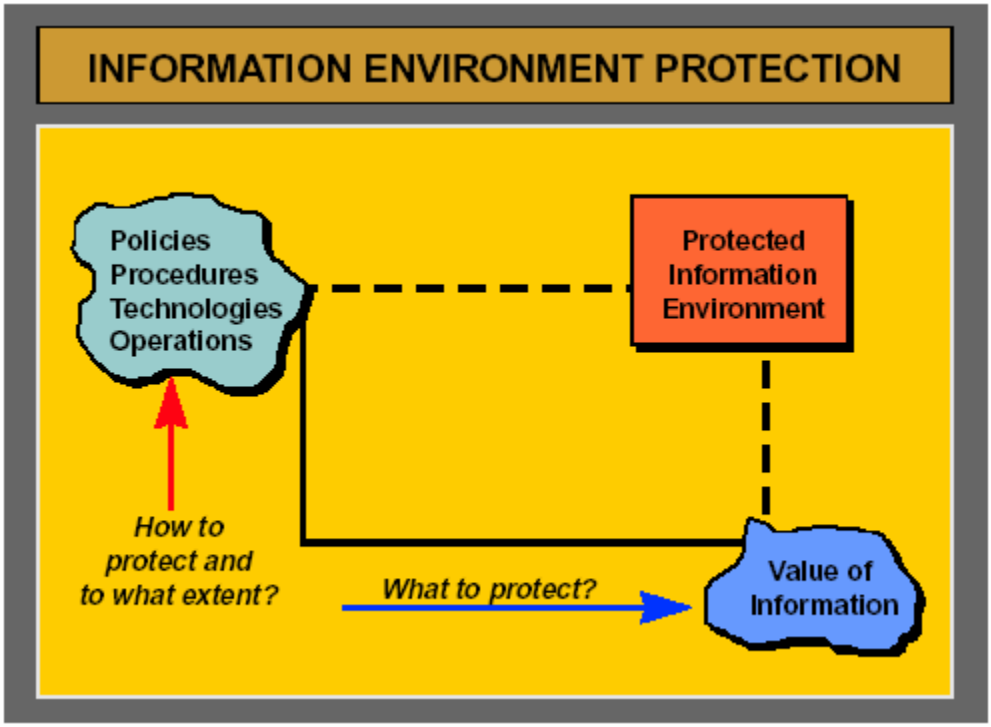

Figure 2. Information Environment Protection (JP 3-13, 1998:III-8)

Vulnerability analysis and assessments are crucial to creating a protected information environment (JP 3-13, 1998:II-9). If a commander does not know where the problems are, he or she will never be able to fix them. Vulnerabilities include threats as widely varied as terrorists (domestic and foreign), disgruntled workers, accidental magnetic emanations, electrical impulses, simple accidents, and natural phenomena such as sunspots, hurricanes and earthquakes (JP 3-13, 1998:II-9). It would be unrealistic to expect a perfect defense against all vulnerabilities of all information. Joint Force Commanders should therefore assess what are their most critical assets, those critical

assets' greatest vulnerabilities, and the best protective measures to be taken against those vulnerabilities.

Service Doctrines

U.S. Army

U.S. Army Field Manual (FM) 100-6, Information Operations, describes IO as the management of the Military Information Environment (MIE) and its links to the Global Information Environment (GIE). These links include, among other things, the media, the Global Information Infrastructure, the National Information Infrastructure, the Defense Information Infrastructure, other governments, and domestic and international organizations. The components to accomplish this are operations, relevant information/intelligence, and information systems (FM 100-6, 1996:2-3). Figure 3 gives an overview of these relationships.

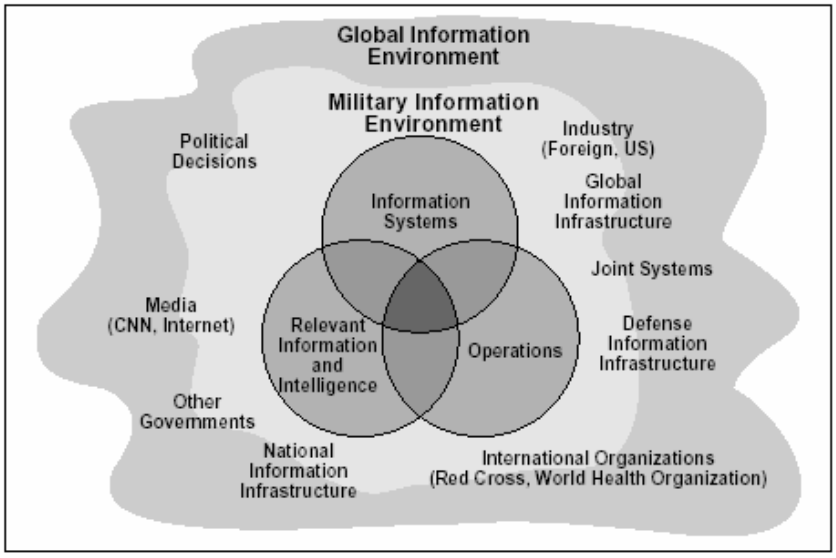

Figure 3. U.S. Army Depiction of Information Operations (FM 100-6, 1996)

Operations that support IO are focused in three areas: command and control warfare (C^2W), civil affairs operations (CA), and public affairs operations (PA). C^2W (a

major emphasis of the U.S. Marine Corps doctrine) is intended to influence, deny information to, degrade, or destroy adversary C^2 capabilities (C^2 attack) protecting C^2 capabilities against such actions (C^2 protect) (FM 100-6, 1996:2-4). CA and PA operations manage the links between the MIE and the GIE in order to provide the best socio-political environment in which to conduct operations. PA operations, recognizing the reality of modern public scrutiny, are focused on the media link. Psychological operations—attempting to influence the mindset of the adversary—are integrated throughout all of these activities. This is a critical factor in the war on terrorism.

Relevant Information and Intelligence (RII) is focused on ensuring that the right people get the right information at the right time—not an easy task with the vast volume of information available with today's technology, and the multiple ways that that information can be corrupted or compromised. Information systems must be designed with the proper architecture and global connectivity in order to link the strategic, operational, and tactical elements of IO into a consistent, coordinated effort (FM 100-6, 1996:2-8).

One of the main functions of information operations is attaining the advantage of having better situational awareness than the enemy. The process of attaining situational awareness starts with data collection from the multitudes of sources (that change constantly). Next, the data are then processed into information, information is then refined into knowledge, and finally, judgment is applied to the knowledge to gain understanding (FM 100-6, 1996:1-11). Figure 4 presents an overview of this process. Unfortunately, our foes have this same "awareness" need. The double-edged sword of IT can cut both ways should a foe penetrate a critical system.

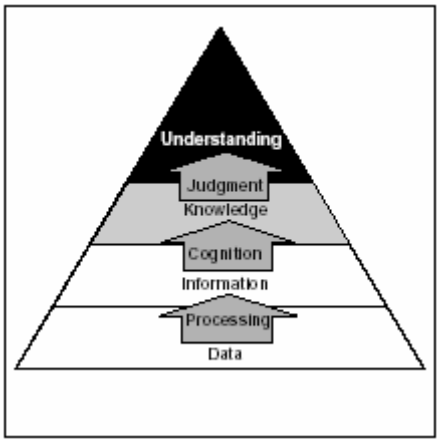

Figure 4. Evolution of Data to Understanding (FM 100-6, 1996)

U.S. Air Force

Air Force Doctrine Document (AFDD) 2-5 is the principle source for understanding the Air Force's perspective on the conduct of information operations. Air Force Doctrine describes information operations as two main activities: information in war (IIW) and information warfare (IW). IIW concentrates on the gaining and exploiting information while IW activities focus on attacking and defending information and information systems (AFDD 2-5, 2002:4). The Air Force conducts both IW and IIW activities throughout the spectrum of conflict from peace to war to peace. Figure 5 illustrates the relationship between IW and IIW. This depiction shows that though specific objectives of IW and IIW are usually different, the activities sometimes overlap.

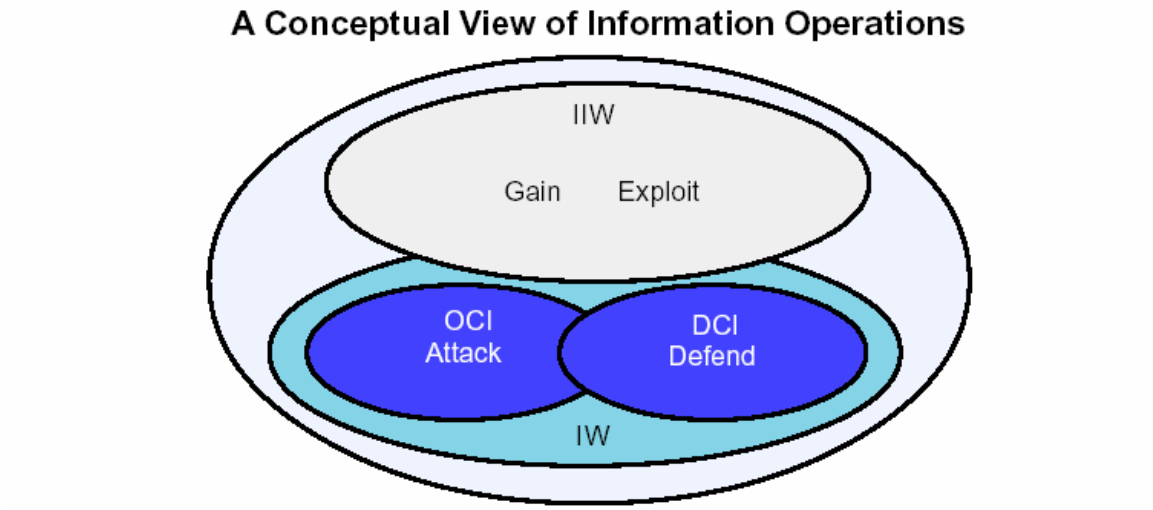

Figure 5. Air Force Doctrine Depiction of Information Operations (AFDD 2-5, 2002)

Information threats can be understood in terms of the "5 D's." Information threats intend to **disrupt, deny, degrade, destroy** or **deceive** information or information systems thus affecting decision making. The potential information threats facing the U.S. are not limited by geographical or political boundaries (AFDD 2-5, 2002:7).

AFDD 2-5 describes IW in different terms than Joint publications. The Air Force defines counterinformation as what the Joint doctrine terms information warfare. In Joint doctrine, information warfare activities occur during hostilities, whereas the Air Force conducts IW activities every day (AFDD 2-5, 2002:11). AFDD 2-5 describes IW in the same terms as other doctrine publications describe air warfare. For example, just as the purpose of offensive counter air is to actively destroy the enemy's ability to wage war in the air, offensive counter information is intent on destroying the enemy's war fighting capability in the information realm (AFDD 2-5, 2002:12).

Offensive counterinformation includes psychological operations (PSYOP), electronic warfare (EW), military deception, physical attack, and computer network

attack. PSYOP is an operational discipline that targets the mind of the adversary. The purpose of PSYOP is to influence the perceptions, attitudes, reasoning, and behavior of adversaries in a manner favorable to military objectives (AFDD 2-5, 2002: 12). Electronic warfare is "any military action involving the use of electromagnetic or directed energy to manipulate the electromagnetic spectrum or to attack an adversary" (AFDD 2-5, 2002:14).

Military deception is simply misleading the adversary into taking actions intended by the deception. Certainly not new to the science and practice of war, deception has always, and will always, be fundamental to warfare. Sun Tzu (1971) wrote over two thousand years ago "All warfare is based on deception." In World War II, the Allies deceived the Germans into thinking the D-Day attack would begin at Calais instead of Normandy. In the Persian Gulf War, placing U.S. Marines off the coast of Kuwait deceived Iraq into preparing for an amphibious invasion that never came; this allowed coalition forces to invade Iraq on their western flank (General H. Norman Schwarzkopf's "Hail Mary" maneuver), catching the Iraqis ill prepared to defend the attack (AFDD 2-5, 2002:16).

Physical attack and computer network attack are both means of intentionally targeting enemy information and information systems. While physical attack uses tangible weapons to disrupt, damage, or destroy an adversary's information or information systems, computer network attacks are conducted via computer or telecommunication systems (AFDD 2-5, 2002: 18). Computer network attacks may be limited to the enemy's information and leave the information systems intact. Both

physical attacks and computer network attacks have the potential to compliment PSYOP activities (AFDD 2-5, 2002:18).

Defensive counterinformation (DCI) operations include operations security (OPSEC), information assurance (IA), computer network defense, counterdeception, counterintelligence, public affairs operations, counter propaganda operations, and electronic warfare (electronic protection) (AFDD 2-5, 2002:21). The purpose of OPSEC is to identify critical components of friendly information, analyze friendly actions that accompany military operations, identify vulnerabilities of friendly activities to enemy intelligence, and develop measures to mitigate those vulnerabilities. OPSEC is a methodology that can be applied to any military operation/activity in order to deny critical information to the enemy (AFDD 2-5, 2002:22). The purpose of IA is to protect and defend friendly information and information systems by ensuring their:

1. Availability
2. Integrity
3. Authenticity
4. Confidentiality
5. Nonrepudiation

Computer Network Defense (CND) is the set of actions taken to plan and direct responses to unauthorized activity in defense of Air Force information systems and computer networks (AFDD 2-5, 2002: 23). Counterdeception is the effort to gain advantage from, negate, neutralize, or diminish the effects of, a foreign deception operation (AFDD 2-5, 2002: 24). Counterintelligence protects operations, information systems, and other resources from illegal clandestine acts by foreign intelligence services, terrorist groups and other adversaries. Counterpropaganda operations are aimed at negating the effects of enemy PSYOP and propaganda efforts. To counter the effects of

propaganda, U.S. and friendly forces must strive to become the favored source of information by the international news media. Credibility and truth are the best weapons in a propaganda operation. The military should be conducting all the activities of DCI throughout the spectrum of conflict.

U.S. Marine Corps

The USMC has not yet published doctrine on Information Operations. Marine Corps Warfighting Pamphlet (MCWP) 3-36 is currently being drafted, and offers a reasonably accurate view of the Marines' approach to IO. Barring any major changes, MCWP 3-36's description of IO will parallel JP 3-13, AFDD 2-5, and FM-100. Similar to JP 3-13, the Marines define Information Warfare as "the conduct of IO during a time of crisis or conflict to achieve or promote specific objectives over a specific adversary. There is no other difference in the scope or method between IW and IO." (MCWP 3-36 draft, 2002:27) Like AFDD 2-5, the Marines' approach to IO is composed of deception, electronic warfare, OPSEC, PSYOP, physical destruction, computer network attack, and computer network defense. The draft of MCWP 3-36 uses very similar language to define those terms (MCWP 3-36 draft, 2002:27-47).

In addition to the draft of MCWP 3-36, Marine Corps Doctrine Pamphlet 6 (MCDP 6) on Command and Control doctrine has a great deal of relevance to IO. In that document, the information hierarchy is described almost exactly like FM 100-6 (raw data becomes processed data which leads to knowledge which leads (hopefully) to understanding) (MCDP 6, 1996:37). Articulating the OODA (observe, orient, decide, and act) loop as the basic sequence of the command and control process, we can see that

information operations are basically protecting the integrity of one's OODA loop while disrupting the adversary's.

Government Reports

In 1997, The White House Commission on Aviation Safety and Security issued its final report and recognized the threat of information operations in that report. While no specific IO vulnerabilities or defensive measures were stated, the Commission recommended, among many other things, that the FAA should establish a high level of protection for all aviation information systems. Essentially the report stated that the government, the airline industry, and airports would have to share the burden of IO defense and that the National Security Agency would "play a role in coordinating information security measures." (Gore, 1997:28)

That same year, the President's Commission on Critical Infrastructure Protection (PCCIP) released its report, *Critical Foundations*, depicting a vast array of information-age threats to the nation's infrastructures. In the area of transportation, the commission noted that the business of transportation was rapidly evolving from an enterprise conducted with paper contracts, bills of lading, manifests and other records to one heavily reliant on paperless electronic records and data processing systems (PCCIP, 1997:A-12). Electronic commerce is transforming the physical distribution industry into one where "just-in-time" logistics is the norm, rather than the exception. This transformation, however, makes the industry increasingly vulnerable to disruption of its electric and communication infrastructures (PCCIP, 1997:A-12).

One major vulnerability that the PCCIP explained in *Critical Foundations* was the trend to rely on the Global Positioning System (GPS) for air navigation. The report

stated that the FAA has a plan to make GPS the sole radio navigation mechanism by 2010. The Commission strongly advised that implementing such a plan makes the air transportation system vulnerable because no single system can be reasonably expected to be 100% reliable (PCCIP, 1997:A-12).

Government Accounting Office (GAO) Reports

In January 2001, President Clinton reported to Congress the status of activities in critical infrastructure protection (CIP). That report outlined Presidential Decision Directive (PDD) 63, articulating a strategy to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of (italics added):

> 1. The Federal Government to perform essential national security missions and to ensure the general public health and safety;
> 2. State and local governments to maintain order and to deliver minimum essential public services; and
> 3. The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and *transportation* services.

PDD-63 delineated responsibilities and programs of the major Federal departments and agencies. The Department of Commerce is the lead agency for information and communications while the Department of Transportation is responsible for airports, highways, mass transit, pipelines, railroads, and seaports (GAO, 2001:5). The directive created the National Coordinator for Security, Critical Infrastructure, a part of the National Security Council (NSC) staff, and Counter-Terrorism as well as the Critical Infrastructure Assurance Office (CIAO), an interagency office housed at the Commerce Department.

The report updates the status of activities, programs, and initiatives of thirteen leading Federal departments' and eight major Federal agencies. The report does not

relate specific accomplishments in improving the nation's posture against physical or cyber threats to the nation's infrastructure, but rather it reports on the efforts to coordinate the actions of government and industry to devise methods to combat those threats. The report alludes to the fact that a "shortage of expert information security personnel" (GAO, 2001:66) has two effects on the governments approach to CIP. First, the government needs to cooperate with the private sector in order to attain the best methodology for countering information-age threats. Second, the widely scattered activities of the federal government need to be coordinated and standardized in order to minimize the overall effort required (GAO, 2001:66).

PDD-63 identified eight major sectors of the economy, appointed a Lead Agency and a Sector Liaison to work with the private sector in order to develop the National Infrastructure Assurance Plan. Those sectors are (italics added):

1. Banking and Finance
2. Energy
3. *Information and Communications*
4. *Transportation*
5. Water Supply
6. Emergency Fire Services and Continuity of Government
7. Emergency Law Enforcement
8. Public Health Services Sector

The lead agency for Information and Communication is the National Telecommunication and Information Administration (NITA), under the Department of Commerce. The lead agency for Transportation is the Department of Transportation (DOT).

NITA's effort to protect the information and communication infrastructure from cyber and physical attack so far consists of:

1. Developing awareness and education;
2. Assisting the information and communication sector in identifying, mitigating and eliminating vulnerabilities;

3. Advancing solutions for the global I&C infrastructure by working with foreign governments, international organizations, and multinational corporations; and
4. Providing industry with information on results from U.S. Government R&D on CIP (GAO, 2001:16).

DOT, on the other hand, has been charged with facilitating and coordinating activities of the private sector owners and operators of the nation's transportation infrastructure. The Department has tentatively identified the following components of the transportation infrastructure as critical:

1. Civil aviation, particularly the National Airspace System;
2. The nation's rail system, focused on command, control, and communications systems;
3. The nation's pipeline transmission systems;
4. The nation's seaports and waterways, including the St. Lawrence Seaway;
5. Defense mobilization critical transportation links, including rail, highway, and ports; and
6. The Global Positioning System (GPS).

It is important to note that in the aftermath of the 11 September terrorist attack, there is an ongoing effort to restructure roles and responsibilities in the context of homeland defense. With the recent establishment of the Transportation Security Administration, the planned creation of a new unified command (U.S. Northern Command), the restructuring of the FBI, and the possibility of making the Director of Homeland Security a cabinet level position subject to Senate confirmation, it is highly likely that tasks under PDD 63 will be shifted and new responsibilities created.

Congressional Testimony

In June 2000, Joel C. Willemssen, Director of the Civil Agencies Information Systems Accounting and Information Management Division, testified before the House Subcommittee on Government Management, Information and Technology on the proposed Cyber Security Act of 2000. The legislation was intended to remove barriers to information sharing between government and private industry in order to better protect the nation's critical infrastructure (Willemssen, 2000:1). In that testimony, Willemssen pointed out that the National Infrastructure Protection Center (NIPC), under the Federal Bureau of Investigation is charged with the mission of collecting information on cyber attacks and other threats to the Information and Communication (I&C) infrastructure. In some cases the NIPC was able to gather information and deter a computer virus attack in a timely manner, but in other cases, they were not. In May of 2000, cyber terrorists released the ILOVEYOU virus which caused over six billion dollars worth of software damage and lost commerce (Abreu). According to Willemssen, the NIPC first learned of the virus at 0545, but did not issue an alert until 1100, after many federal agencies were already infected.

Mr. Willemssen also had strong reservations about the federal government's ability to enforce computer security. He stated that,

> "…our audits have repeatedly identified serious deficiencies in the most basic controls over access to federal systems. For example, managers often provided overly broad access privileges to very large groups of users, affording far more individuals than necessary the ability to browse, and sometimes modify or delete, sensitive or critical information. In addition, access was often not appropriately authorized or documented; users often shared accounts and passwords or posted passwords in plain view; software access controls were improperly implemented; and user

> activity was not adequately monitored to deter and identify inappropriate actions." (Willemssen, 2000:9)

In July 2000, Jack L. Brock, Jr., Director of the Governmentwide and Defense Information Systems Accounting and Information Management Division, testified on the challenges to building a comprehensive strategy for Information Sharing and Coordination. Like Mr. Willemssen, he stated the need for close coordination between all the users of information technology in order to develop "comprehensive and practical approaches and solutions to these threats" (Brock, 2000:2). Brock stated that the threat of destructive computer viruses was growing substantially; in 1993, 10% of known viruses were destructive, but in 2000 that number had grown to 35% (Brock, 2000:2). He noted audits conducted by the GAO that revealed that 22 of the largest federal agencies had serious computer security weakness. The cause of these weaknesses, according to Brock, could be partially attributed to insufficient understanding of risks and technical staff shortages, but was primarily a fundamental problem of poor security program management (Brock, 2000:10).

Mr. Brock pointed to a study of organizations with superior security programs that indicated an effective framework for dealing information security. That framework is a risk management cycle which (1) assesses risk and determines protection needs, (2) selects and implements cost-effective policies and controls to meet these needs, (3) promotes awareness of policies and controls and of the risks that prompted their adoption, and (4) implements a program of routine tests and examinations for evaluating the effectiveness of policies and related controls (Brock, 2000:11).

Commercial Perspectives on Information Assurance Research

Sponsored by the National Security Agency, the Institute for Defense Analyses conducted a study published in 1997 for the PCCIP. The major findings of that study (primarily relying on interviews) include:

1. U.S. commercial information assurance R&D is fairly robust but lacking in depth. Industry is actively researching multiple aspects of IA (base hardware, operating systems protection, network protocols, security management, etc.). What the authors claim, however, is that any given area of research may involve only five or six companies. While this is good for achieving consensus, the approach fails to generate sufficient ideas attainable from more in-depth research (Mayfield et al., 1997:8).
2. Part of industry's problem is "shaping" customer demand. Technology providers cannot wait for customer demand—they must increase the customers' awareness of the needs regarding information assurance (Mayfield et al., 1997:10).
3. Several areas need more funding/emphasis. The most critical problem in IA research, and according to the study's findings, the one not being pursued, is system-level security engineering (Mayfield et al., 1997:24). Industry needs system-level security architectures that enable secure interoperability among heterogeneous components (Mayfield et al., 1997:26). Availability and integrity were identified as the two biggest technology problems urgently requiring both

research and product development (Mayfield et al., 1997:28).

Industry, government, and academia need to develop stronger ties; partnerships and alliances will facilitate better implementation of IA technologies, and application programming interfaces are needed to promote technology transfer (Mayfield et al., 1997:30).

4. U.S. export control is restraining IA R&D. The study cites unnamed sources who estimate that $2 billion would be invested annually if export controls on IA technology were lifted (Mayfield et al., 1997:33).
5. Commercial industry believes that it must solve the IA problem for critical infrastructures, but it will not do so without a larger degree of government leadership, motivation and facilitation (Mayfield et al., 1997:37).

Journal Publications/Periodicals/Other Published Research

The RAND research institution conducted a study sponsored by the National Security Agency, the Defense Advanced Research Projects Agency, and the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence aimed at articulating the concept of a "minimum essential information infrastructure" (MEII). The MEII concept is patterned after the Minimum Essential Emergency Communication Network (MEECN) established during the Cold War for use during a nuclear attack (Anderson and Gritton, 1999: 2). In that study, the authors identified twenty information system vulnerabilities in seven categories (design, behavior, adaptability, configuration,

nonphysical exposure, physical exposure, and supporting infrastructures). (Anderson and Gritton, 1999:30-35) These vulnerabilities are reproduced in Table 1.

Table 1. Categories of System Vulnerabilities
(Anderson, 1999: xvi)

Vulnerability	A system or process:
Inherent design/architecture	
Uniqueness	That is unique and may be less likely to have been thoroughly tested and perfected
Singularity	Representing a single point of failure, or even acting as a "lightning rod" for attacks
Centralization	In which all decisions, data, and control must pass through a central node or process
Separability	That is easily isolated from the rest of the system
Homogeneity	In which a flaw may be widely replicated in multiple, identical instances
Behavioral complexity	
Sensitivity	That is especially sensitive to variations in user input or abnormal use—an attribute that can be exploited
Predictability	Having external behavior that is predictable; attackers can know the results their actions will have
Adaptability and manipulation	
Rigidity	That cannot easily be changed in response to an attack, or made to adapt automatically under attack
Malleability	That is easily modifiable
Gullibility	That is easy to fool
Operation/configuration	
Capacity limits	Near capacity limits that may be vulnerable to denial-of service attacks
Lack of recoverability	Requiring inordinate time or effort to recover operation, relative to requirements
Lack of self-awareness	That is unable to monitor its own use
Difficulty of management	That is difficult to configure and maintain, so known flaws may not be found or fixed
Complacency/co-optability	With poor administrative procedures, insufficient screening of operators, etc.
Indirect/nonphysical exposure	
Electronic accessibility	For which remote access provides an attack opening
Transparency	That allows an attacker to gain information about it
Direct/physical exposure	
Physical accessibility	In which attackers can get close enough to system components to do physical damage
Electromagnetic susceptibility	In which attackers can get close enough to use radiated energy to disable a system
Supporting facilities/infrastructures	
Dependency	That depends on information feeds, power, etc.

The study compared these vulnerabilities against the 22 most severe computer attacks reported to the CERT® Coordination Center from 1989-1995 and found that all of the attacks exploited nine of the twenty vulnerabilities (homogeneity, predictability, malleability, gullibility, lack of self-awareness, difficulty of management, complacency and co-optability, electronic accessibility, and transparency). Of these nine, the authors conclude that homogeneity (identical instances of a logical entity that requires the malicious logic to be created just once then applied to multiple targets) and transparency (openness to the public that makes discovery of flaws easier) are the most pervasive vulnerabilities. A noteworthy conclusion that the authors made was that systems that have poor reliability would make better assets for an MEII. This is because systems that fail frequently will force users to develop alternative ways to work around them (Anderson and Gritton, 1999:45).

Signal Magazine, a trade journal of communications, electronics, intelligence, and information systems professionals, published an article in 1999 discussing the threats to the U.S. information infrastructure. According to the article, U.S. security may be severely threatened by internal software or hardware trapdoors lying dormant in the nation's critical infrastructure (Ackerman, 1999). According to Richard A. Clarke, National Coordinator for Security, Infrastructure Protection and Counterterrorism at the National Security Council, the U.S. has become so dependent on computer networks that without them, "there is no water coming out of your tap; there is no electricity lighting your room; there is no food being transported to your grocery store; there is no money coming out of your bank; there is no 911 system responding to emergencies; there is no Army, Navy, and Air Force defending the country." (Ackerman, 1999)

Mr. Clarke further states that the year 2000 (Y2K) phenomenon taught business and government just how dependent the government was on functioning computer networks. If a potential system malfunction such as Y2K, that was not created by a hostile actor, could threaten the country with such catastrophic damage, what might happen when an adversary intentionally inflicts the same damage feared by Y2K? Clarke describes trapdoors as malicious computer code that can be used to make a computer malfunction. If activated in the right way, these trap doors could disrupt the operation of multiple critical infrastructures simultaneously (Ackerman, 1999).

MIT's *Technology Review* posted an article from the *Atlanta Journal-Constitution* describing an experiment where a computer security consultant demonstrated how easy it is to access information at an airport. From a parked car, using a laptop computer and $125 in attachments, the consultant was able to hack in to the airline's central computer by receiving signals emitted by wireless systems operated by agents at the airport's curbside check-in (Plummer, 2002). The consultant, Bill Corbitt, a former Air Force computer security officer, claimed that he or a terrorist could read airline e-mails, discover who was going where, find out how much fuel was being uploaded, and even clear bomb-laden baggage through security (Plummer, 2002). Many businesses are becoming increasingly reliant on wireless technology because of its convenience and efficiency; that convenience, unfortunately, comes from technology that has the potential to make system information more vulnerable. Mr. Corbitt claims he was able to locate 120 wireless portals and discovered only 32 of them had even activated the encryption software, which he further claims can usually be cracked relatively easily (Plummer, 2002).

Carnegie Mellon University's CERT® Coordination Center posted a report on 8 April 2002 depicting the following trends in computer intruder activity:

1. The level of automation is continually increasing; scanning patterns are more advanced and can self-initiate new attack cycles.
2. The tools used in computer attack are increasingly more sophisticated; they are more difficult to discover and detect; anti-virus software is increasingly less effective.
3. Vulnerabilities are being discovered at a faster rate; the number of newly discovered vulnerabilities more than doubles each year; the speed of discovering vulnerabilities is rapidly outpacing the ability of software developers and customers to patch the vulnerabilities.
4. Firewalls are becoming decreasingly effective; the development of firewall and anti-firewall software is rapidly spiraling out of control (Carnegie Mellon University, 2002).

All of this points to increases in potential susceptibilities and vulnerabilities in the interface of military and civilian operations.

Interviews with Experts

Retired General Walter Kross, President and CEO of Flight Explorer, a company specializing in aviation-industry software, was the Commander in Chief of USTRANSCOM from 1996-1998. He, along with Mr. Charles Beard, the Managing Director for Aerospace at KPMG Consulting, also a retired Air Force officer, gave an interview to the author on 15 May 2002. The following is a synopsis of their comments

on IO vulnerabilities of commercial airlines performing contract/CRAF (Civil Reserve Air Fleet) flights for TRANSOCM.

According to General Kross and Mr. Beard, the airlines' biggest IO vulnerability is the physical integrity of their automated flight scheduling system and reservation system. Enough critical information is kept off the Internet that cyber attacks would probably be less effective, and would require direct access to the appropriate local area network (LAN). The actual flight scheduling system is a very crucial node to the operation of the airline as a whole. Destroying that system by a physical attack would potentially cause chaos in the carriers' ability to operate a smoothly flowing schedule. Though the TRANSCOM flights are going to be charter flights, and can be tracked independently, the planes and crews used for those flights are tracked by the flight scheduling system. The crews will also be shifting from passenger flights to charter flights and need to be tracked. Many flight crews "deadhead" (fly as passengers to where they can be used as crew members) and need to be tracked. Without the flight scheduling system, whether physically or electronically attacked, crew and aircraft flow will be disrupted. Disrupting the civilian business will most assuredly affect the military business. Though the contracted flights would eventually be completed, the resulting delay would bring havoc to the military's deployment flow.

Airline operations are controlled by operations centers, organized and equipped according to the airline's business practices. These operations centers are the focal point of commanding and controlling the planes and crews. Vital flight information (flight plans, manifests, weather, maintenance requirement, and so forth) is collected and communicated to the crews, mechanics, gate agents and other employees who keep the

system moving. Taking out these operations centers, by whatever direct or indirect means, would cripple the airlines' ability to maintain their schedule. Again, any disruption in flight schedules would affect crew availabilities and has a high potential of affecting military airlift.

Civilian airline crews are vulnerable to PSYOP. Many crew members are former military servicemen or part-time Reservists and, as General Kross points out, are enthusiastic and patriotic about their role in the Defense Transportation System. Still, the reality is that civilians require a higher level of safety than military personnel. Threats, or perceived threats, to that safety are a potential vulnerability to an airline's ability to operate. General Kross reflected from his role as Director of Operations and Logistics for TRANSCOM during the Persian Gulf War that CRAF aircrews were occasionally reluctant to fly out of concern for their safety after receiving news of Iraqi SCUD missile attacks. Mr. Beard mentioned that crews congregating at airport hotels normally use an airline's facility information portal to keep informed of issues from the operations center. Reports of civilian airline crews being assassinated aboard shuttle buses that carry them to the airport, or white powder resembling weaponized anthrax found on an airplane, would likely cause many crews to not fly.

In summary, the review of available literature indicates that information technology is a vulnerable target for destruction and degradation. Industry and government both share a common reliance on similar, and often the exact same, infrastructures. Those infrastructures need to be examined and vulnerabilities mitigated.

This has been a review of open-source documents, but is not intended to be all-inclusive. Vulnerabilities do indeed exist, but the knowledge of them, in addition to the sources and methods used to obtain that knowledge, must be protected from disclosure.

III. Methodology

Developing a methodology for examining the information operation vulnerabilities of commercial air carriers is a challenging undertaking. It requires analyzing the process of procuring the services of commercial air carriers, the process of transferring passengers and cargo to the carrier, and the operation of the airports, commercial and military. Coupled with this, a specific threat analysis is required. In the context of how information operations is understood by the military today, this paper attempts to hypothesize how a potential adversary might disrupt, deny, degrade, destroy or deceive the information or information systems involved in this system.

Operational Dependency Matrix

One methodology for examining the effects of disruptions in commercial infrastructures on mission effectiveness is an Operational Dependency Matrix. Provided by the Joint Program Office for Special Technologies Countermeasures (JPO-STC), the matrix is a useful tool for translating "outside the fence" disruptions into operational, quantifiable impacts. First, the analyst must decide what system is to be examined (for example, a fast-food restaurant, a military base, a commercial airport, a hub-and-spoke airline, a major unified command). The next step is to list the most critical missions of that system—those missions that fulfill the very purpose of the system's existence. Next the analyst should develop a list of functions required to fulfill each mission and a list of tasks required to enable each function. Many functions are common to multiple missions and need only be listed once. Likewise, many tasks are common to multiple functions and should also be listed just once. The last step in developing the matrix is to examine

the major infrastructures (energy, transportation, and communication) and all the components of these infrastructures.

To use the matrix, the analyst would try to determine what tasks would be unfeasible in the event of a hypothetical failure of a particular element of the infrastructure (the base telephone switching station, for example). Knowing what tasks cannot be completed then reveals which functions are infeasible which in turn shows which missions are vulnerable to failure. Figure 6 shows a notional example of an Operational Dependency Matrix and how this tool is used to aid the analysis. The example shows a failure of electrical power (EP) affecting a task, which affects a function, which affects Mission A.

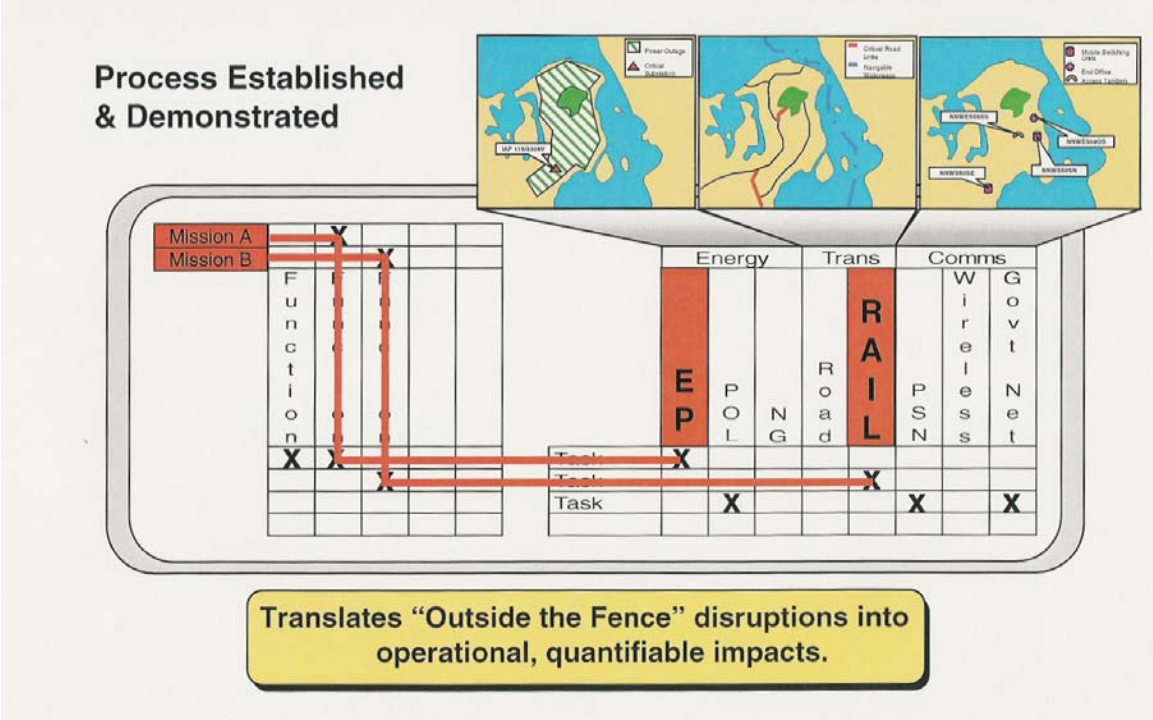

Figure 6. Operational Dependency Matrix (JPO-STC, 2001)

Analyzing Contract Airlift

The system of interest in this study starts with a Theater CINC validating a requirement for transportation of troops or equipment. TRANSCOM takes the validated requirement and forwards it via the Defense Message Transfer System (DMTS) to the appropriate component command (AMC for airlift, Military Sealift Command for sealift, or Military Traffic Management Command for truck and rail). In the case of airlift, AMC tasks its airlift wings to carry as much of the lift requirement as they can manage (cargo classified as "outsized" must be carried by AMC as the cargo can only fit on a C-5 or C-17, or a rarely used Ukrainian Antonov AN-124). As mentioned in the introduction, AMC's lift capacity is usually insufficient for a major deployment. The remainder of the lift requirement is offered/advertised to commercial contract carriers for bidding. According to Mr. Tom Boschert, a GS-12 at AMC's Tanker Airlift Control Center (TACC), the "bidding" is not like and auction, because the rates are negotiated and set by a different process. The request for offers is done via unclassified e-mail to carriers who wish to be notified of potential business. If the requirement is short notice (five days or less), AMC's Contract Airlift Division (AMC/DOY) calls carriers directly in a method similar to a freight broker in the trucking industry. Data for the mission, including the user, the passengers and cargo, the origin and destination, are stored in a database called COINS. Though COINS is used only by personnel in AMC, data from COINS are posted on an unclassified electronic bulletin board and routinely transmitted on e-mail messages.

IO vulnerabilities at this stage of procuring the work from the airline are the systems and links between AMC and the carriers. The servers at HQ AMC, the

telephone lines that AMC would use if there Internet connections go down, and the power supply system need to keep the communication open are all vulnerable. According to Mr. Larry Pasek, the Deputy Base Civil Engineer at Scott AFB, electrical power to the base is supplied by Illinois Power and generated off base. Though the security of the base itself may be outstanding, the base and its infrastructure are vulnerable to an attack on power supplies the military may not have the ability or authority to protect during normal operations. Mr. Pasek states that at Scott AFB, diesel generators are in place to supply power to the base's critical functions in the event of commercial power failure. A civilian air depot would require similar facilities and sufficient backup power to assure a timely, effective changeover.

The high volume of military communication transmitted over civilian lines and through civilian computer network servers between AMC and commercial air carriers creates a variety of susceptibilities. Messages could be changed, creating confusion on the part of the commercial airlines as they attempt to bid and perform contracts that are different from AMC's requirement. Messages could be deleted entirely, forcing added hours of work in securing lift that would have been coordinated sooner, had the airlines been notified. Finally, false messages could be transmitted causing carriers to bid on non-existent missions, tie up the operation with effort sorting out the mess, and possibly eroding the carriers' desire to do business with AMC. Worse, critical supplies and forces might be misdirected or misrouted.

Independent of the initial contract offer and acceptance activity, the combat units being transported are responsible to move their equipment and people to the aerial port of embarkation (APOE). This process is one of the most vulnerable to OPSEC degradation.

The flurry of activity involved with preparing conventional forces for deployment is likely to generate news/media coverage, cellular phone calls, unclassified conversations and other sources of information that intelligence agents will be able to monitor.

As for delivering loads to the contract carrier, information technology is vital to rapidly processing the volumes of data into load plans. Crews use these plans to ensure that the planes are aerodynamically balanced and that they have sufficient fuel to carry the load to the aerial port of debarkation (APOD). In most cases the military will do load plans at the APOE and provide them to the carrier; AMC aerial port personnel have manuals and software for planning loads for both military and commercial aircraft. Disrupting or destroying the automation of load plans/weight and balance data would have a debilitating effect on maintaining a smooth flow of aircraft departures. Furthermore, if a malevolent actor were crafty enough, he or she might be able to cause a plane to be loaded out of limits and crash.

Arguably, the most critical place to look for IO vulnerabilities in commercial airline operations is at the airports. Though much of the contract charter flights will be loaded away from the larger commercial hubs (Atlanta, New York, LAX), the volume of traffic through these nodes make these airports lucrative "dual effect" targets where civilian and military transportation would be disrupted simultaneously. If an enemy can cause enough havoc at these major airports, it would be like draining the oil from a finely tuned engine; the motor (the airline) would seize and would be unable to function effectively for TRANSCOM.

Analyzing an airport's infrastructure is an enormous undertaking. In anticipation of potential Y2K-related computer failures, airport managers around the country

performed various levels of analysis to examine their facilities' vulnerability to computer failure. Taking those reports off the shelf, finding a best-practices model of infrastructure inspection, and examining those same information infrastructures for both physical and cyber attacks, coupled with a valid risk assessment, should produce a useful picture of vulnerabilities.

A visit to the AMC passenger service detachment at Baltimore-Washington International (BWI) airport revealed several interesting facts and potential vulnerabilities. According to MSgt Sharon Kegler, superintendent of Detachment 1 of the 305th Aerial Port Squadron (APS), BWI serves as an APOE for over 170,000 passengers per year traveling on AMC contract flights across the Atlantic. Commercial carriers such as American Trans Air, Omni, and World Airways support AMC's movement of troops overseas, including 75% of passengers rotating on Aerospace Expeditionary Force deployments, from BWI.

Information flow between 305 APS Det 1, AMC Headquarters, and commercial carriers is depicted in Figure 7. The Det at BWI does not deal directly with the carriers but rather with AMC. AMC's Directorate of Operations (DO) tasks the Contract Airlift Division (DOY) with awarding contracts to the carriers. Once the missions are planned, AMC uses the Global Decision Support System (GDSS) to track all airlift (military and contract) missions. At BWI, Det 1 updates the Global Air Transportation Execution System (GATES), which is linked to GDSS and TRANSCOM's Global Transportation Network (GTN). GTN is an Internet website where TRANSCOM's customers can log in and see the status of their shipments. This collection of unclassified systems is susceptible to disruption, degradation, and destruction.

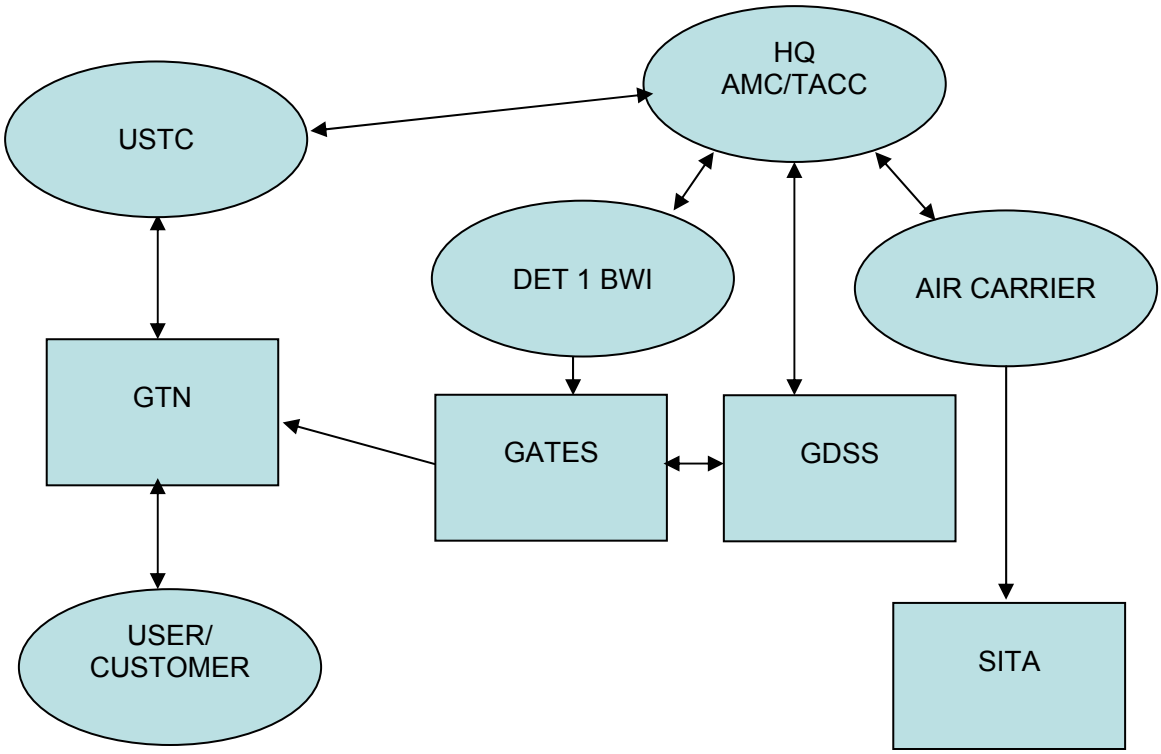

Figure 7. Information Flow for AMC Operations at BWI

According to Justus Heger, Operations Representative for World Airways, all commercial carriers have relied on electronic data transfer for communications for decades. Messages are transmitted by virtually every carrier in "SITA text." Data transmission services are provided by primarily two companies, SITA and Air Inc. Mr. Heger further states that the SITA text messages are transmitted via computer modem on a closed encrypted network from the airports to a central server, which processes all messages for all major carriers. Those messages can also be transmitted to Internet e-mail accounts as Mr. Heger demonstrated by sending the author a departure message for an AMC contract flight departing BWI for Frankfurt. Destroying this server, and its backups, would probably force the carriers to use less efficient means of communication, again showing another potential opportunity for a foe to hinder operations.

Compromising the system would also create the potential for enemy deception. Worse, such a compromise might result in the loss of operational data critical to a foe's operations against U.S. or allied forces. Up to date intelligence of flight manifests, departures, and arrivals would be invaluable in planning and executing operations against these flights, whether by direct military action, guerilla operations, terrorist attacks, or a combination of such activities.

Risk Assessment

In order to mitigate these IO threats against the commercial airline operations, government and industry will need to work together to accomplish a valid risk analysis of the information infrastructure. Just as the Department of Defense performs IA security audits with risk assessments on its military facilities, commercial air carriers and airports should do the same for commercial facilities and their interfaces with DoD systems. A basic framework for risk assessment is shown in Figure 8.

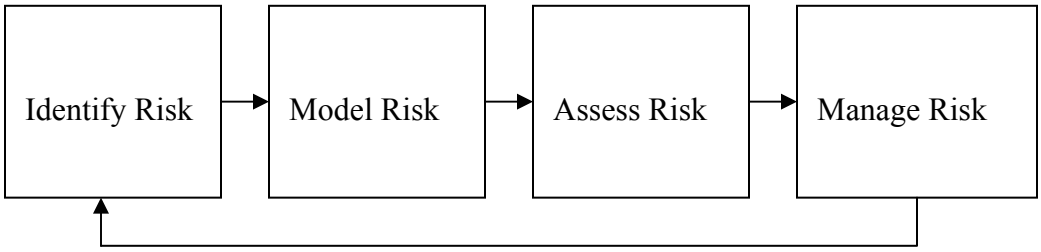

Figure 8. Risk Management Framework (Ezell et al., 2001:24)

The objective of risk assessment is not to make every component of a system perfectly fortified against all possible attacks, but rather to identify the most serious and most likely risks (using probability of occurrence and a valid quantitative measure of damage) and mitigate those. A tradeoff analysis will then allow the decision makers to decide how

much time, effort, and money to spend on mitigating vulnerabilities and how much risk they are willing to assume by not defending against every possible threat (Ezell, et al., 2001: 24).

Figure 9, based on the principles in the DoD auditors guidelines, suggests an overview of a potential mitigation approach. Combining an evaluation of potential vulnerabilities and susceptibilities, developed perhaps with a modification of the Operational Dependency Matrix with an appropriate risk assessment, as outlined by Ezell et al, will provide a mechanism to realistically evaluate and manage the threat. The combination of the potential risk, coupled with measures of its negative effects, will provide a method for ranking potential vulnerabilities and to apply controls to mitigate those vulnerabilities.

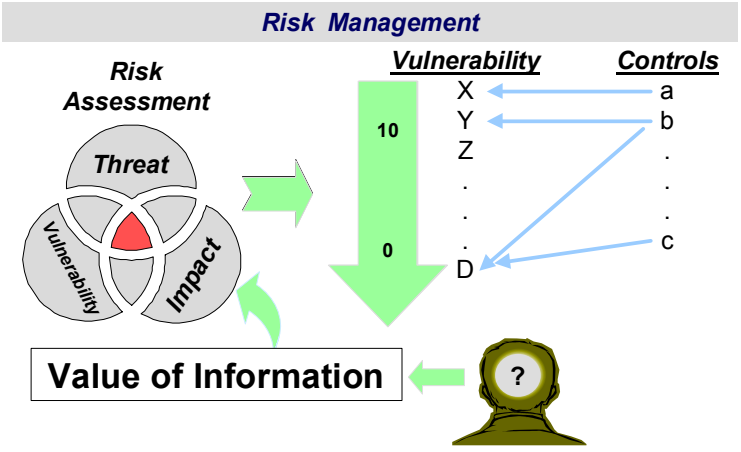

Figure 9. Risk Management and the Value of Information Model (Hamill, 2000:3-23)

Such an assessment must recognize the mission-essential and OPSEC consideration of a movement. As a chain is no stronger than its weakest link, the analysis must include both the civilian and military aspects of the system. Tradeoffs will, nevertheless, have to be made, as it is impossible to defend everywhere. A detailed risk

management system can, however, will assist in making those tradeoffs. While the service CERT's do provide threat assessments and Red Team analysis, the civilian sector, while benefiting from the CERT and FBI reports currently available, do not have full access to all the resources available to the DoD. In addition, risk and threat assessments do require funding.

Summary

These audits and assessment will enable TRANSCOM and the DoD to decide how much security is needed in the commercial aviation infrastructure and how much it will cost to attain that security. The military cannot dictate business practices to the private sector; however, with Congressional support, the military can strongly encourage businesses to comply with minimum desired IA safeguards by not awarding contracts to firms that refuse to comply. IA standards can be established and these ratings can be used to stratify what size contracts an airline can compete for. Deciding on these issues is a critical command and political decision that must be resolved to continue the current war on terrorism and to develop a new strategy for homeland defense.

IV. Conclusions and Discussion

Information Operations represent a very real threat to commercial airlines conducting flights as part of USTRANSCOM's mission to rapidly deploy forces executing the nation's military operations. The volume of commercial airlift required to augment Air Mobility Command's military airlift fleet make the operation of commercial air carriers a vital necessity to national security. By that fact, the commercial airlines are a vulnerable target for enemy action; if the enemy can keep the airlines from moving forces to the fight, the results could be the same as if the enemy had won the fight on the battlefield.

There are two primary information operations threats to the critical infrastructures of commercial air transportation—physical threats and cyber threats to information and information systems. Of these two, the threats to the physical assets required to process information necessary appear to be more serious; though the potential for damage caused by cyber threats is serious and well documented, the ability to destroy or incapacitate those systems requires less effort and the results would probably be more effective. Though PDD 63 and the activities of the PCCIP are steering the nation in the right direction, more research is needed to develop valid protections for the nation's critical infrastructures. The basic approach to this research is to answer the following questions:

1. What are the critical infrastructures?
2. What are the most severe vulnerabilities?
3. How should the vulnerabilities be mitigated?

While developing defensive countermeasures to IO threats is important, policy makers should consider mitigating threatening adversaries' abilities to attack the

information systems of the United States (using lethal force when necessary). Countermeasures will only work until technology is developed to defeat them, and research shows that this innovative technology is being developed at a rapidly increasing rate. IT security will be a constant technological challenge for the future. The effort required to effectively accomplish this is enormous, but the resulting security will be worth the effort, and the cost of not making these assessments would be devastating.

References

Abreu, Elinor. *"New email virus may hurt worse than 'Love.'"* 12 May 2000 (online). Available: http://www.cnn.com/2000/TECH/computing/05/12/new.love.virus.idg/

Ackerman, Robert K. "Hidden Hazards Menace U.S. Information Infrastructure." *Signal Magazine*, August 1999 (online). Available: http://www.us.net/signal/Archive/August99/hidden-aug.html

Anderson, Robert H. and Gritton, Eugene C. *Securing the U.S. Defense Information Infrastructure: a Proposed Approach.* Santa Monica, CA: Rand, 1999.

Beard, Charles. Managing Director for Aerospace, KPMG Consulting, McLean, VA. Telephone Interview. 15 May 2002.

Boschert, John T. Special Assignment Airlift Mission Director, Tanker Airlift Control Center, Scott Air Force Base, IL. Telephone Interview. 17 December 2001.

Brock, Jack L., Jr. "*Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination*" (Congressional Testimony). 26 July 2000.

Carnegie Mellon University. *Overview of Attack Trends*. 8 April 2002 (online). Available: http://www.cert.org/archive/pdf/attack_trends.pdf.

Cunningham, William. Class lecture, LOGM 617, Strategic Transportation. School of Operational Sciences, Air Force Institute of Technology, Ft Dix, NJ, November 2001.

Department of the Air Force. *Information Operations*. AFDD 2-5. Washington: HQ USAF, 4 Jan 2002.

Department of the Army: *Information Operations*. FM 100-6. Washington: HQ USA, August 1996.

Department of Defense. *Joint Doctrine for Information Operations*. Joint Publication 3-13. Washington: GPO, 9 October 1998.

Department of the Navy. *Command and Control*. Marine Corps Doctrine Pamphlet 6. Quantico, VA: USMC Doctrine Center, 4 Oct 1996.

Department of the Navy. *Information Operations (Draft)*. Marine Corps Warfighting Pamphlet 3-36. Not dated.

Ezell, Barry C. et al. "Risks of Cyber Attack to Water Utility Supervisory Control and Data Acquisition Systems," *Military Operations Research*, 6: 23-33 (June 2001).

Fisher, Uri. "Information Age State Security: New Threats to Old Boundaries." *Journal of Homeland Security*, November 2001 (online). Available: http://www.homelandsecurity.org/journal/articles/display/Article.asp?article=25.

Gore, Al. Final Report: *White House Commission on Aviation Safety and Security*. 12 Feb 1997.

GAO. *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities*. January 2001.

Hamill, Jonathan T. et al. "Risk Management and the Value of Information in a Defense Computer System." Unpublished Report. Air Force Institute of Technology. Wright-Patterson AFB, OH, 28 March 2002.

Hamill, Jonathan T. *Modeling Information Assurance: A Value Focused Thinking Approach.* MS Thesis, AFIT/GOR/ENS/00M-15. School of Operational Sciences, Air Force Institute of Technology (AU), Wright-Patterson AFB, OH, March 2000.

Heger, Justus. Operations Representative, World Airways, Baltimore, MD. Personal Interview, 20 May 2002.

Henry, Martin. Air Force Representative, Joint Program Office for Special Technologies Countermeasures, Dahlgren VA. Personal Interview,

Joint Program Office for Special Technologies Countermeasures (JPO-STC). "US Infrastructure Assurance Supporting Military Operations." Unpublished Report. Dahlgren, VA, 2001.

Joint Vision 2020. U.S. Government Printing Office. June 2000.

Kegler, Sharon L. MSgt, USAF. Superintendent, Detachment 1, 305th Aerial Port Squadron, Baltimore, MD. Personal Interview, 20 May 2002.

Kross, Walter. President and CEO, Flight Explorer, Fairfax, VA. Telephone interview. 15 May 2002.

Mayfield, William T. et. al. "*Commercial Perspectives on Information Assurance Research*." Alexandria, VA: Institute for Defense Analyses, 1998.

Plummer, Don. *Wireless Systems Simple to Hack*: Consultant Shows How Easy. Atlanta Journal-Constitution, 31 March 2002 (online). Available: http://www.techreview.com/offthewire/3001_142002_4.asp

President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures*. Washington: U.S Government Printing Office, October 1997.

Sun Tzu. *The Art of War*. New York: Oxford University Press, 1971.

USTRANSCOM J3/4-BC. *Transportation for a New Millennium: 2000 Annual Command Report*. Scott AFB, IL: HQ USTC, Spring 2001.

Willemssen, Joel C. *Comments on the Proposed Cyber Security Act of 2000* (Congressional Testimony). Government Accounting Office, GAO/T-AIMD-00-229: 22 June 2000

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
07 06 2002	Graduate Research Paper	May 2001 - Jun 2002

4. TITLE AND SUBTITLE

Commercial Air Carrier Vulnerabilities to Information Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Shelburn, Bryan H., Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GMO/ENS/02E-11

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

USTRANSCOM/TCJ3-OD
Colonel Kathy Gainey
508 Scott Drive
Scott AFB, IL 62225-5357

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

The conduct of Information Operations by the United States Military and its enemies is changing because of the rapid development of information technology. The increasing dependence of government and industry on information technology has created critical vulnerabilities that can be exploited by degrading or destroying the use of information systems. Among those elements susceptible to these vulnerabilities are the operations of commercial air carriers that are essential to the military's ability to wage war and project power wherever needed in the world. These threats must be seriously examined and mitigated to ensure that commercial air carriers can fulfill their roles in our national security strategy.

This study reveals potential Information Operations vulnerabilities in the commercial air carriers' conduct of missions for the military. The systems used by Air Mobility Command to plan and track the operation of contracted airlift, and those used by the airlines to operate their flight schedule, are susceptible to physical and cyber attacks. A potential result of a successful attack is a dramatic slowdown in the operation of commercial air carriers that could lead to unacceptable delays in transporting combat forces where they are needed to execute national military objectives.

15. SUBJECT TERMS

Information Operations, Commercial Air Transportation, Critical Infrastructure Protection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Richard F. Deckro
U	U	U	UU	52	19b. TELEPHONE NUMBER *(include area code)* (937) 255-6565 x4325