5-2000

Information warfare and modern aircraft

Gregory E. Hauser

To the Graduate Council:

I am submitting herewith a thesis written by Gregory E. Hauser entitled "Information warfare and modern aircraft." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Aviation Systems.

C. T. N. Paludan, Major Professor

We have read this thesis and recommend its acceptance:

Frank S. Collins

Accepted for the Council:
Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:

I am submitting herewith a thesis written by Gregory E. Hauser entitled "Information Warfare and Modern Aircraft". I have examined the final copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Aviation Systems.

C. T. N. Paludan

Dr. C. T. N Paludan, Major Professor

We have read this thesis
and recommend its acceptance:

Alfonso Pujol Jr

Frank G. Collins

Accepted for the Council:

Associate Vice Chancellor
and Dean of The Graduate School

INFORMATION WARFARE AND MODERN AIRCRAFT

A Thesis

Presented for the Master of Science

Degree

The University of Tennessee, Knoxville

Gregory E. Hauser

May 2000

DEDICATION

This thesis is dedicated to my wife and children

Angeles

Stephanie, Curtis and Ryan

ABSTRACT

The purpose of this thesis is to determine if modern aircraft are currently at risk of falling victim to information warfare attacks or if they will be in the near future (less than 10 years). Defensive measures that are currently being used to protect this critical infrastructure will be discussed and evaluated for their effectiveness in preventing the degradation caused by these attacks.

Every effort has been made to use reliable sources of information to present an accurate status of modern aircraft and the aviation infrastructure with respect to information warfare. With information warfare being such a recent topic, much of the most up-to-date information has not been published in traditional medium yet and therefore, the author had to augment his research by utilizing "other sources", such as newspaper articles, magazines and the Internet.

It was concluded that, to date, neither the airline industry nor the FAA has experienced large-scale attacks by cyber warriors, even though the industry is becoming more susceptible to such attacks This absence of attacks SHOULD NOT BE used to lull oneself into a false sense of security with the conclusion that the industry is properly protected from information warfare attacks. The reality is that these information warfare attacks can and are being successfully executed at an extreme cost and/or danger to the ill prepared and lucrative targets.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

The author is a military pilot, and is most interested in investigating and evaluating the current and near term state (within 10 years) of both commercial and military aircraft with respect to information warfare and the threat it presents to the aviation infrastructure As we fly into this new era that-has been dubbed a revolution in military affairs (RMA), which does not apply only to the military, are proper precautions being taken to avoid falling victim of our own advanced technology in the form of information warfare?

Modern aircraft have not been the target of extensive information warfare attacks, but with their increasing use of information systems the possibilities must be considered. In order to draw conclusions on the vulnerability of modern aircraft with respect to information warfare, other areas such as the U.S. military and the financial sector will be closely evaluated These two other sectors have taken the bulk of the costly information warfare attacks to date and therefore can provide valuable insight into the future of information warfare and how it could affect modern aircraft.

In order to fully understand the current situation, it is most important to know the background of how and why technology took the route it did with respect to information systems. Today, economic pressures are the driving forces behind the increasing

employment of advanced technology to increase efficiency and remain competitive. Chapter II will ensure the reader of this thesis obtains a good basic understanding of information warfare and realizes its full potential. Finally, Chapter II will present the current situation of information warfare and give examples of costly information warfare attacks.

Offense information warfare will be completely covered in Chapter III, as this must be addressed before defensive measures can be properly analyzed. The basic concepts and the weapons of offensive information warfare will be presented first, in order to be able to properly explain how information warfare attacks can affect airliners. Chapter IV, defensive information warfare, will concentrate on methods of defending airliners from these attacks

Every effort has been made to use reliable sources of information to present an accurate status of modern aircraft and the aviation infrastructure with respect to information warfare. Information warfare is such a recent topic that much of the most up-to-date information has not been published in books yet and therefore the author had to augment his research by utilizing "other sources". Limiting the research material to traditional sources, such as printed books, would only allow this thesis to present a historical view, which in many cases is very different than the actual situation. Newspaper articles, magazines and the Internet were all used to obtain information on events that have not made it into more formal references yet. Appendices A, B and C demonstrate the

quantity and quality of these "other sources. With few exceptions, the "information" contained in the sub-levels of Appendix B are official government documents, articles/papers sponsored by reputable universities, Think-tanks, or by reputable authors/experts in the field The authenticity of information found in the Internet is always subject to questioning and the utmost care was taken to only utilize authentic sources

To summarize, the purpose of this thesis is to determine if modern aircraft are currently at risk of falling victim to information warfare attacks or if they will be in the near future. Defensive measures that are currently being used to protect this critical infrastructure will be discussed and evaluated for their effectiveness in preventing the degradation caused by these attacks.

The author has never worked with nor had first hand knowledge of any military activities related to information warfare until he was directed to write a thesis for the Command and Staff school on "Information Warfare". All information in his military thesis that he presented in June of 1999, was unclassified and collected from unclassified sources.

CHAPTER II

BACKGROUND, BASICS AND EXAMPLES

Information Systems

The rapid advancements in technology over the past 20 years have brought about the information age, in which data and information can be manipulated and utilized to drastically increase the digital capacity of sophisticated equipment Today, 49% of households in the United States have computer access, with a large portion of them also having access to the Internet and these percentages are rapidly increasing. As it becomes obvious that computers and information access is no longer just a "nice to have" in the business world, but rather a vital requirement, the rate of increase in the number of computers with Internet access globally is staggering The National information infrastructure (NII) is a subset of the larger Global information infrastructure (GII), both of which are the backbones for communications, telecommunications, commerce, media, navigation and network services It is estimated that in 1996 the GII was valued at $1 trillion and the NII at $500 billion (18). Each one of these computers that make up the GII and NII can be viewed as an access port to a whole New World of information or as a base of operations for information warfare

"Being Connected", No longer just a Nice To Have

The need for information systems extends further than just a computer, as a system can become much more valuable if it is "Connected" to the External World. Computers were designed to rapidly manipulate data and return *useful* information. The degree to which a computer can return useful information is directly proportional to the volume of relevant information and sources the system can access. For example, a computer that is used in a department store can be used as a fancy adding machine or, if it is allowed access to the Universal Product Codes (UPC) and the corresponding prices, the computer can be used as an efficient cash register. Now, if it were given access to stock figures, the computer could be used to generate new orders when the stock becomes low and give management many useful products to more effectively control stock and observe customer trends.

In this same way, the use of computers in modern aircraft is restricted if they are not allowed to digitally communicate externally to the aircraft. These restrictions can turn a high-speed aircraft computer into only a sophisticated navigation computer or a complex autopilot, rather than a complex information management and communication system. The more external sources providing relevant information will increase the potential utility of the onboard computers Currently, the airline industry can use these data links to access a variety of essential information to more efficiently manage their aircraft. This information can include, but is not limited to, weather information, destinations/departure conditions similar to Airport Terminal Information Service (ATIS), gate information, and

sports scores, which seems to be a very popular thing for the pilots to announce. The flight dispatcher and maintenance department can receive information, such as the exact location and flight conditions of the aircraft that they are managing, the aircraft maintenance condition prior to landing, etc

The next logical step in the near future for the Federal Aviation Administrations (FAA) is to be digitally connected to aircraft via a data link system. Flight clearances could be passed as well as the Air Traffic Controllers (ATC) could continuously monitor flight data as well as aircraft data. A network such as this could enhance safety as well as more efficiently control the flow of aircraft. Every year there are aircraft mishaps where a contributing factor is a misunderstanding in communications caused by a language barrier or just poor communications (human or equipment induced). A tragic example of this was in 1990, when a B 707 ran out of fuel in New York after holding for over 1 hour because the pilot miscommunicated his fuel state and did not use proper terminology. This could have been easily avoided if the controllers could have monitored the aircraft's fuel state or the foreign pilot had conveyed his status clearly.

As seen from the above, the commercial airline industry can not avoid to adopt these new communication capabilities that technology has offered and therefore the future promises to bring an increase to the volume of digital information traffic that modern commercial aircraft must process to remain competitive. Along with these advancements will come the possible problems and risks associated with becoming dependent on computers and

information based systems. Historically, aircraft were closed systems, meaning aircraft operated without outside information/data being received or transmitted from the aircraft, with the exception of voice transmissions. These "access ports" are where this information must enter the aircraft's information system and they will be thoroughly discussed from the standpoint of security. Currently, the military is extensively utilizing these data links in modern aircraft to enhance their potential and without a doubt, commercial airlines companies will soon begin to employ them to more efficiently and safely manage their aircraft fleets.

As more airplanes (private, commercial, corporate and military) take to the airways, the management of this airspace becomes more critical. The precise control of these aircraft must be maintained continuously in order to keep the efficient, safe flow of aircraft. With the advent of high speed/capacity computers and the nation wide network of radar, the required "safety bubble" around aircraft under instrument flight rules (IFR) has been reduced allowing for a higher density of airborne aircraft. Though more aircraft are taking to the air every year, their destinations/transfer points, for the most part, remain the same, thereby causing even greater problems in and around major metropolitan centers such as Los Angeles, San Francisco, Washington DC, Saint Louis, Denver, Chicago, Miami etc In order to funnel the extensive volume of traffic into and out of a relatively small area, the use of computers is vital. Even though the thrust of this thesis is the vulnerability of aircraft to information warfare attacks, the air traffic control system's

reliance on modern computers must be considered also, as its incapacitation could reduce the flow of traffic to a trickle.

Who is in Control?

Until the late 1980's, the military was paving the way for these new technologic advancements and the civilian community received the spin-off technology as they could not afford, nor had reason to fund the tremendous up front cost of this basic R&D. As the defense budgets shrunk due to the ending of the cold war and the civilian information systems sector began to expand rapidly, the civilian community took the lead in these high technology markets. In 1994, the Secretary of Defense, William J. Perry (SECDEF) changed the course of the United States military acquisition system and has attempted to streamline the acquisition cycle (22). Prior to this SECDEF policy decision, the military had to adhere to very strict "military standards" (MILSTD), that drastically slowed down the acceptance of new technology and ensured that the military was obtaining well proven antiquated equipment. This decision allowed the military to utilize commercially available products instead of investing vast sums of money into R&D that was already being accomplished by the civilian sector. These commercial off the shelf products (COTS) include, but are not limited to, micro chips, computers and network systems that are now being installed as the brains of new military hardware such as aircraft, ships and tanks.

When the military developed the Internet and was in control of the technology and hardware that support this massive network, it was very easy to prevent unauthorized access. Since the late 80's, the military is no longer in control of these markets and there are few governmental controls on the utilization or distributions of this technology, which has directly lead to the present situation. For a price, virtually anything can be legally acquired as long as it does not possess inherent destructive capabilities.

The military has been experiencing costly devastating information warfare attacks for years now and has just begun to control this problem. It is important to grasp the concept that an aircraft connected to a network is nothing more than just another node on the network and therefore, it is just as vulnerable as any other node on the network if extensive precautions are not taken onboard the aircraft. As the civilian sector moves rapidly into this information age, where information is money and power, the quantity and cost of these attacks is bound to increase also

The military is leading the way in utilizing commercial off the shelf equipment (COTS) for advanced integration designs and advanced communications equipment. By the author's estimates, the military is about 10 years more advanced than the civilian sector with respect to integrated computing power in large vehicles (Naval, Aircraft and Land). Therefore, in order to evaluate future civilian equipment with respect to integration, it is important to examine current and planned military equipment as they are paving the way

for the civilian markets. This advanced technology is taking both the civilian and military communities into uncharted waters, where the size and number of obstacles (threats) are unknown.

Digital Communication

A data link is the connection between two computers that are not normally co-located for the purpose of transmitting and receiving digital information over an established communication's link. This link can utilize many different media to propagate the data/information that vary from telephone lines to radio frequency (RF) transmissions (VLF to SHF) to light. The factor that limits the amount of information that can be transmitted over a given media is the bandwidth of the signal which is carrying the information and as a general rule, as the carrier frequency increases, the available bandwidth also increases. The following equation was developed by Nyquist in 1924 and shows the relationship between bandwidth and maximum data rate (assuming no noise) (6).

$$\text{Max data rate} = 2\,H \log_2 V \text{ bits/sec}$$

Where H is the bandwidth of the signal
V is discrete levels (2 for binary data)

Example: with a bandwidth of 3kHz the maximum data rate for a digital signal would be 6k bits/sec or 6k bps

From this equation, it is easy to see that the higher the frequency of the signal, the larger the bandwidth and therefore higher data rates can be successfully propagated over the communication link. This is demonstrated by the extremely slow data rates (100 bps) that submarines have when they are forced to utilize VLF (10kHz) due to mission requirements (submerged). On the USAF E-3, AWACS communicates with other national assets via a SHF (1 GHz) data link at data rates in the range of 1Mbps, but normally, additional channels are added so multiple streams of data can share the bandwidth (9).

The Military's Usage of Data Links for Mobile Platforms

The military has been using data links for years now, with great success in aircraft. Most modern military combat aircraft are being designed with data links for a variety of missions or the aircraft are being retrofitted with this data link capability. Fighter-to-fighter data links are no longer just a nice-to-have but are becoming a requirement in order to share radar pictures and targeting information with other fighters, early warning aircraft, and ships. Attack aircraft are currently extensively employing these data links to pass and receive targeting information from friendly troops on the ground or airborne targeting aircraft. The ground side of the military is utilizing data links more than the tactical airborne platforms are, with great success. The future of the military is sure to

bring a continued expansion to the number and volume of digital data being passed among military units, regardless if they are tactical or strategic, fixed or mobile, airborne, ground or sea based. There is no reason to think that the civilian market will not move in this direction

The digital data transmission with tactical aircraft can be encrypted if the particular situation so dictates In the near future when the threat becomes more sophisticated with the aid of high technology made widely available by COTS equipment at affordable prices, there will be a need to encrypt all digital communication

Airlines and Digital Communication

At present, there are a few different systems on the commercial market that offer digital data communications specifically designed for commercial airliner. Aeronautical Radio Incorporated markets a bi-directional data link, which operates in the VHF frequency band (9). It is capable of automatic transfer of operational data and maintenance reports between onboard systems and ground based computers. This system is in service with many Airbus and Boeing aircraft today. As the above system operates in a Line Of Sight frequency band, the utility is limited to less than 200 miles from a transmitter station (7). HF data links also exist that can have world wide coverage at reduced data rates,

AlliedSignal Commercial Avionics Systems produces a system that is certified for flight on American Airlines Boeing 767-300 aircraft (9).

As airline companies and the FAA quickly capitalize on this new technology that the information age has delivered, extreme caution must be used when implementing system to ensure that the vulnerability to information warfare attacks are minimized and critical subsystems are well protected from such attacks. The two primary end users of this technology are.

- The FAA. Aircraft and controllers in the future will most likely use these data link in order to maintain constant digital communication between the ground controller and the aircraft, for such things as position keeping and aircraft routing and clearance
- Airliner's ground support team (dispatchers and maintenance personnel) These lines of communication will be used to keep the dispatcher FULLY informed on the position and status of the aircraft. The maintenance personnel will be able to more effectively prepare for "turning around" the aircraft for the next flight by knowing the maintenance condition of the aircraft prior to it landing and pulling into the gate

The two basic methods of establishing digital communications with an airborne aircraft are via the use of land based transmitters in the radio frequency (RF) band or via a satellite communication link (21) Both methods have their advantages and disadvantages, for example:

- Land based direct communications.
    - Transmitters are less expensive.
    - Frequency selection is critical as Very High Frequency (VHF, 30-150 MHz) band that offers a line of sight maximum range of approximately 200 NM and would therefore require an extensive network of transmitter sites if large area were to be covered by the system. If High Frequency (HF, 2-30 MHz) were

employed, the bandwidth would reduce the data rate possibly to an unacceptable level.

- Satellite communication.
    - Requires leased satellite time, as it is unlikely that any one airline company would desire to operate their own satellites for communications.
    - Possibly more costly than direct land communications with respect to: money/bits of information
    - Worldwide coverage.
    - High data rates if VHF/UHF or SHF were to be utilized.

Currently, commercial aircraft are equipped with VHF radios for short-range communications, mostly over land and HF radios for long range communications, which is mostly over water. The only satellite signals that are currently being received by most airliners are those of a satellite's navigation system. The author postulates that, as satellite communications cost continues to drop, airline companies will opt for satellite communications, as it requires the lowest up front cost for a data link to its fleet of aircraft. Probably between 2010 and 2020, the FAA will set up a VHF/UHF "internet" type network that would allow all participating aircraft to "log on to" and could be used to digital communicate with the FAA, as well as the airliner's flight dispatchers.

Information Warfare

Information warfare is so new that the definition is different in almost every source, but the essence of most definitions is the same: the interruption or corruption of the flow of information with the intent to deny, degrade or exploit the capacity of a civilian or military system. The part exploit "without permission" is a large part of information warfare, as it is nothing more than stealing information. In the past, stealing industrial secrets or private information normally meant stealing printed material or photographing something, but now it can be accomplished in the digital world for possible illicit purposes. This more traditional crime will not be the focus of this thesis as it is the same old crime, only with a new medium to operate in.

The above definition of information warfare includes the following groups of persons, many of them not directly related to the topic of this thesis, but it is important for the reader to have a thorough grasp of "what information warfare is" in all of its new and different forms:

- *Insiders*: are employees, former employees, temporaries, contractors and any other person or group that has been granted access through security of a given system. This group is generally considered to be an organization's largest threat (2). They may be selling trade secrets to a foreign government, selling sensitive information to a competitor or information broker, etc.

- *Hackers*: A hacker is someone who, for a variety of reasons, breaks into computer systems. These actions can be "just for fun", challenge, ideology, revenge, power, the financial reward may or may not be a motivator of the hacker. Even when they not intended to damage a system or release information, the hacking damages the integrity of a system and is a time/assess waster for the system administrator.

- *Criminal.* The criminal element is normally financially motivated and therefore most of their targets are financial institutions such as bank accounts/passwords, credit card numbers or any other digital product that can be easily exchanged for money. Though many may not consider information warfare attacks to include pirates of software, CDs or music, these pirates are stealing and exploiting digital information.

- *Corporations*: Corporations may engage in information warfare by collecting information (industrial espionage) on their competitors, such as corporate secrets or by just illegally monitoring their message traffic in order to stay "one step ahead" of them

- *Terrorists*: Terrorists (state sponsored or non-state sponsored) could be considered the most dangerous group listed above, as their intent might include doing massive damage to the critical infrastructure of a country, such as "crashing" Wall Street or cutting off the electrical power in winter to a large portion of the United States To date, there have been few reported cases of cyber-terrorist attacks, but with the proliferation of computers and technology, the number is bound to increase.

- *Governments.* Governments can engage in offensive information warfare legally sanctioned by the government, such as the military during time of war, or illegally. The targets of these attacks can be foreign governments, terrorist groups or any other organization or individual seen as a threat with targets vulnerable to information warfare attacks.

There is no intent to make this thesis sound like a military report by extensively using military terms/acronyms and examples, but the reality is that Information Warfare is a form of "war" and in most situations the military terms are the appropriate ones. A Revolution in Military Affairs (RMA) is when there is a discontinuity in the normal progression of technologic advances, for example, when the artillery or nuclear weapons were first introduced (Figure 2-1). These were not just small steps forwards, but rather large discontinuous jumps, where employing the previous way of thinking was no longer applicable with respect to these new technologies. The majority of sources are in

agreement that the information revolution that started in the 1970's has brought about the current RMA, where not only the rules and actors have changed but also the battlegrounds These battlegrounds of war and terrorism were once restricted to the physical terrain, where the battles were fought, but now, with these new weapons, the battles can take place in "cyberspace" where the number of targets has greatly increased and the stakes of each battle can be much higher.

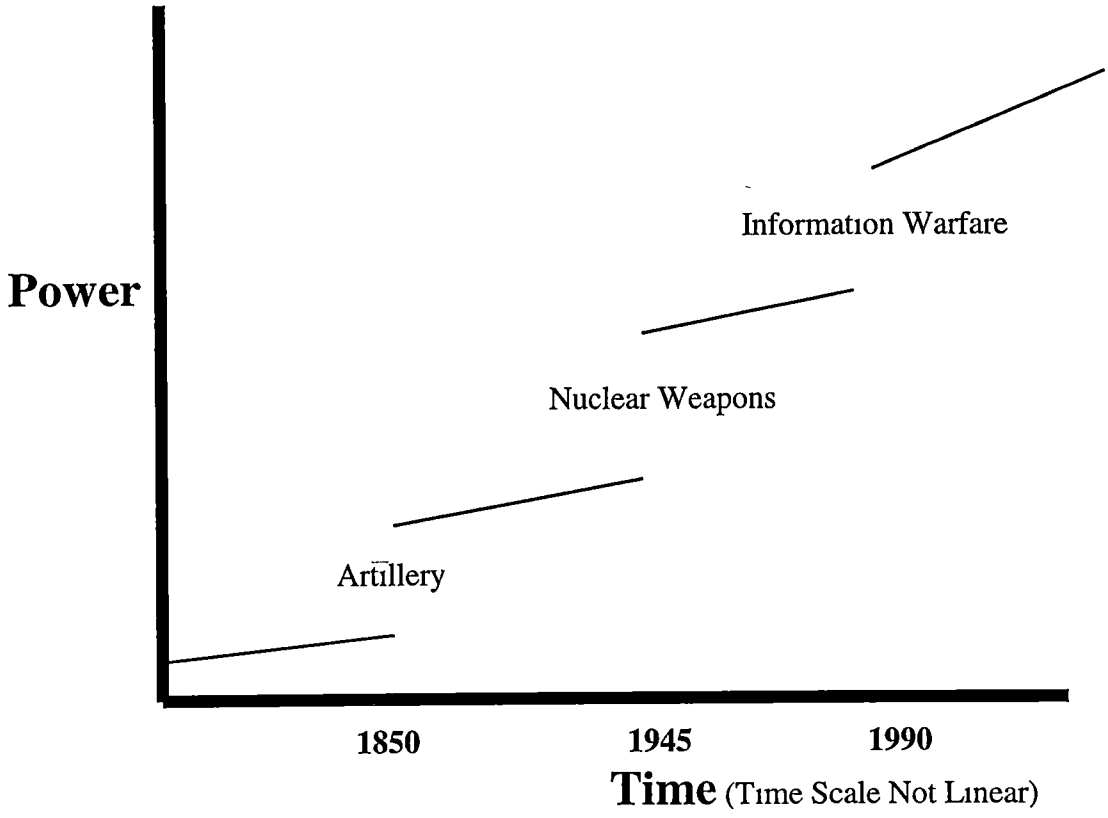

Figure 2-1. Revolution in Military Affairs

Levels of Information Warfare

The following example is given to demonstrate why many people, to include the author, feel that information warfare can be one of the most dangerous weapons a country or group can possess and should be considered a "weapon of mass destruction" (WMD) Nuclear weapons are extremely powerful, but their use by most countries in the civilized world is considered unacceptable and therefore their applications is more as a deterrent than an offensive weapon. The use of nuclear weapons by one country or group will most

likely cause a polarization in opposition to that group or country. This fact alone will most likely keep *Pandora* in her box for years to come On the contrary, information warfare weapons will likely be considered an acceptable form, as the *direct* lethality of these attacks is relativity low, if not zero. The targets of information warfare attacks are not people but rather systems. Consider a communication satellite (data and voice) which is used by the FAA for various things to include passing aircraft information (hand off) from one sector to another or to the next country as it proceeds on route. This satellite could be considered a valid military target, as well as a choice target for a terrorist group. The satellite could be attacked in many different ways, in order to cause different degrees of damage The following is to demonstrate the wide variety of effects/forms an attack could have·

- Level one: The satellite could be simply attacked and disabled or destroyed, thereby denying the use of the satellite. In this example it could reduce significantly the flow of air traffic. Only a very limited number of countries posses weapons to conduct this type of attack.

- Level two: The satellite signals can be intercepted and used to the interceptor's advantage.

- Level three: Part of the satellite's signal can be altered giving a false perception of reality, thereby causing inappropriate decisions to be made. Once again, only a limited number of countries posses weapons to conduct this type of attack.

- Level four· The satellite communications connections can be used as an "access port" into the information infrastructure of those that utilize the satellite For a moment consider that the satellite offers unrestricted access to FAA's main air traffic control computers. The extensive damage and chaos caused by an attack like this could incapacitate a country for years.

The information era has delivered these new more powerful weapons that can be launched virtually anonymously from almost anywhere in the world. With access to the Internet or simply access to a company's telephone remote access and the ability to bypass the company's electronic security measures, everything that is stored on the computers can be put at risk.

The Current Situation

As discussed earlier, information warfare attacks can be conducted by governments, criminals, terrorists (state sponsored or radical group), corporations or individuals, all with the objective of obtaining their goals or bettering their situation. These goals can be strategic, tactical, or "just for fun", but the end result is normally one of two functions, that of capturing (stealing) or affecting information.

Due to information warfare being such a recent development, the legal system has not had time to catch up and therefore, very few laws exist to govern these types of crime. Ethics and morality are insufficient to properly govern this Brave New World that information systems has brought about No longer are size and strength important factors on this battlefield, as now all participating parties have the same opportunities to participate. Human nature and competitiveness have repeatedly shown their ugly heads in the past

and only serve to reinforce the idea that the legal system must be used to enforce civility with respect to information systems.

The tactics and techniques used in the civilian world are identical as to those used in the military with respect to information warfare. The military, no longer having a corner (control) on the "high tech market", coupled with the dramatic reduction in the cost of computing power, has created the present situation in which the software, technology and hardware are all virtually within the reach of anyone.

Do not think that information warfare is only a theory that is rarely encountered in the world today. On the contrary, according to the Government Accounting Office's (GAO) Report 96-84, it was estimated there were 250,000 attacks against DOD's information infrastructure in 1996 alone. This is an annual increase of 100% from the year prior and the success rate of these penetrations was 65% (23). The following is used to support the idea that information warfare attacks are on the rise and these attacks are becoming more lethal and costly:

- A study conducted in 1998 by the Computer Security Institute showed that 64% of those companies surveyed experienced breaches in their information security systems (16% increase over 1996). The total economic loss of the 241 companies was $136,822,000, which represents a 36% increase over 1996 (16)

- A study of 300 Australian companies by Deloitte Touche Tohmatsu revealed that more than 37% of the companies in the survey experienced some type of security problem in 1997, and that the percentage was 57% in banking and finance industries (16).

- In a conference of information security experts in Ottawa, Canada, in the beginning of 1997, it was estimated that the economy of the United States losses $100,000,000,000 every year due to industrial espionage. This is a 500% increase from 1992 (16)

The Computer Security Institute (CSI) (ref. 20) conducted the fourth annual "Computer Crime and Security Survey", in conjunction with the FBI. The results indicate that defensive information warfare practices in use today are not sufficient to defend the robust information infrastructure currently being used in the United States. This survey was directed at 521 well established large companies, most with over 5000 employees from all sectors of the economy (manufacturing, financial, telecommunications, high-tech, medical, government, etc.) Over half the respondents had gross incomes over $500 million. Highlights of this 1999 report are:

- System penetration by outsiders increased for the third year in a row, 30% of the respondents' reported intrusions.
- Those reporting their Internet connection as a "frequent point of attack", rose for the third year, from 37% in 1996 to 57% in 1999.
- Unauthorized access by insiders rose to 55% of respondents reporting incidents of this type
- 32% of respondents did report serious incidents to law enforcement this year.
- A staggering 62% of respondents reported breaches in computer security within the past 12 months.
- Breaking down these breaches into the specific target of the attack, the following is the percentage of respondents that experienced losses in each area

Theft of proprietary information	20%
Sabotage of data or networks	15%
Telecom Eavesdropping	10%
Insider abuse of net access	76%

Financial fraud	11%
Denial of service	25%
Unauthorized access by insiders	43%
Telecom. Fraud	13%
System penetration by outsiders	24%
Virus contamination	70%

It is obvious from the above number that computer crime is NOT on the decrease and more emphasis must be put on defensive measures in order to combat these assaults on the GII and NII

Actual Examples of Costly Information Warfare Attacks

The following examples are presented to demonstrate that even when the industry standard security measures are properly implemented, the persistent "devious criminal minds" can find a way to *break in* and circumvent security measures. It will also be used to show how ineffective the legal system is with respect to information warfare. The United States military has learned some very costly lessons that are also shown here.

During the Gulf War, 5 Dutch information pirates penetrated 34 United States military sites via the Internet between April 1990 and May 1991. They obtained information about the exact locations of American troops and their equipment. This information also included the classified capabilities of the Patriot missile and the movements of war ships

in the region. When they finished their intrusions, they were able to erase any trace that a breach of security took place. When they entered a military logistic system network, they could have changed the logistic support requests for combat units in the gulf from bullets to toilet paper. The pirates tried to sell the information to an Iraqi attaché, but fearing a trap, the attaché did not complete the deal When the pirates were located, they could NOT be convicted, much less tried for anything, as it was not illegal in Holland at that time. The FBI did almost successfully lure them to the United States, where they could have been tried (2).

On 26 March 1999, a virus called Melissa immobilized millions of computers worldwide. During the conflict in Yugoslavia, the NATO server at Aviano airbase, Italy, from where most of the air strikes were launched, was completely shut down for 48 hours (11 and 13).

On 07 April 1999, the NATO home page was disabled after it was attacked by information warfare The attack was most likely launched from Yugoslavia, but the exact attacker was never known or at least never released publicly (observed by author).

A Chinese born computer worker, on Wright Patterson Air Force Base, was discovered viewing and possibly altering highly classified data. Cox News Service reported this on 12 April 1999 The data was maintenance and reliability data on the B-2 bomber and the F-16, which is used as a database for many different classified programs The real risk is

not that the data was compromised by a foreign government, but rather that a dormant virus was planted in the data that can be activated at a more opportune time to contaminate other programs that utilize this data in their data bases. Due to the absolute ineffectiveness of the U S. legal system in these matters, the programmer was sentenced to pay a $5,000 fine and serve the maximum sentence possible for the crime of 6 months (12 and 15)

A Chinese born worker at Los Alamos national laboratories in New Mexico has been under suspicion for 2 years by the FBI for improper disclosure of top secret nuclear weapons data over an extended period of time. The worker admitted moving the data from a highly secured/classified computer to an unclassified computer, where he could more easily access the information This unclassified computer also had direct Internet access and could have sent this data to unauthorized foreign government. Los Alamos laboratories sends out more than 250,000 emails per week, that according to newspaper articles, are too many to possibly be monitored. If this case is true, it demonstrates that there are truly no "cyber-police", as what was given away were some of the United State's most closely guarded secrets.

Private industry seems to be considerably less willing to publicly report the specifics of information warfare attacks, as the United States government is forced to under the freedom of information act It can be assumed from the standpoint of private industry that, if the details are released regarding information warfare attacks, the number of "copy

cat perpetrators" might increase, thereby increasing losses and decreasing public confidence in the network The technology used to execute these break-ins is neither classified nor difficult to obtain. There are various organizations and magazines such as "2600" or "Hackers Quarterly" that openly show in detail how to circumvent information system's security measures. This same information can also be acquired on the Internet from one of many web sites that offer tips and step by step instructions on how to break into systems, two good examples are the following web sites:

alt.2600 QnA

alt.2600.hackerz

CHAPTER III

OFFENSIVE INFORMATION WARFARE

A complete understanding of offensive information warfare is necessary before defensive information warfare can be comprehended, much less defensive measures developed The following introduction to offensive information warfare is designed to demonstrate that along with the new technology surrounding information systems, lies the technology to attack these systems

The DOD has conducted many studies concerning 21st century technology and the Joint Chief of Staff (JCS) has recently developed the "Joint Vision 2000" (JV2000) plan, to guide the United States military well into the next century. In this document, the Chairman of the JCS, General John M Shalikashvili, makes it very clear that the United States military intends to exploit both, offensive and defensive information warfare, as a valid "weapon" of modern warfare (19).

> "Throughout history, gathering, exploiting, and protecting information have been critical in command, control, and intelligence The unqualified importance of information will not change in 2010. What will differ is the increased access to information and improvements in the speed and accuracy of prioritizing and transferring data brought about by advances in technology. While the friction and the fog of war can never be eliminated, new technology promises to mitigate their impact Sustaining the responsive, high quality data processing and information needed for joint military operations will require more than just an edge over an adversary

> We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority will require both offensive and defensive information warfare. Offensive information warfare will degrade or exploit an adversary's collection or use of information. It will include both traditional methods, such as a precision attack to destroy an adversary's command and control capability, as well as nontraditional methods such as electronic intrusion into an information network to convince, confuse, or deceive enemy military decision makers."
>
> General John M. Shalikashvili,
> May 1996

These same words could have been used by a terrorist group, hacker or foreign state, all with the objective of exploiting others' use of information systems.

Basic Concepts of Offensive Information Warfare

Before dividing up the different types of attacks into different groups, the fundamentals of offensive information warfare must be addressed. There exist 7 major characteristics of offensive information warfare attacks and are as follows:

- Function. The intent of the operation normally is capturing or affecting the information. Capturing of the information in many situations can be considered stealing. An example of capturing information would be breaking into the FAA's computers to obtain the exact location of Air Force One while airborne. A similar example, but rather than just *innocently* capturing, could be altering the flight path of an airliner in an effort to have them coincide with that of Air Force One.

- Tactics. The process used to plan and execute the attack in order to obtain the specific objective

- Technique. The technical specifics of the attack that is to be executed.

- Motive. The underlying reason for the information warfare attack The motive can greatly vary and it would be impossible to list, much less know all of them, but the most common are: greed, revenge, ideology, challenge or simply malice. The attacks that are conducted by motives of "just for fun" can be the most difficult to defend against.

- Passive or active. A passive attack is one in which things are observed to gather only information, while an active attack is one in which *things* are touched or altered. An example of passive attack of a large airline company's restricted information areas could be as simple as entering into the access program and observing "authorized users" while entering their user names and passwords, for use later. An active attack with the same function could be an assault on the system administrator's files in order to steal the passwords

- Effect. This is the End State of the attack as seen from the point of view of the victim.

- Legality/Morality. With the speed of new advances in technology, the legal system has not been able to catch up and write effective enforceable laws. This has left us in the current situation where today, few laws exist and even fewer are effective in controlling criminal activity in *cyber-space.* Before the current information era began, it was much simpler to define stealing. Stealing documents or a piece of machinery from one's safe was **stealing.** Today is viewing the email traffic for corporate secrets or even just asking 100 different engineers for harmless information with the purpose of compiling the results to figure out what the corporate competition's next move will be, are these really stealing, is it even unethical or is it just competitiveness?

Weapons of Offensive Information Warfare

The munitions of information warfare are analogues to the cannonballs of a cannon with many major exceptions. The destructive weapons of information warfare can virtually be fired from anywhere in the world anonymously. Conventional, nuclear, biological, and chemical weapons have a maximum effective range and lethal radius, whereas weapons of

information warfare have neither Crafty, highly sophisticated new weapons can be designed and engineered rapidly with equipment that is readily available in an average computer store Traditional weapons are considered to be non-discriminate weapons as they do not differentiate between friendly or enemy, anything within the lethal range will be destroyed equally. This is not true for information weapons, which can be programmed to attack only computers with particular address extensions, for example those of ***gov*** or ***.faa***

The following are the classical information warfare weapons, Figure 3-1 is a wire diagram of these weapons:

- Bacteria. A bacteria is an independent, self-replicating agent program that can create many different versions of itself. It grows at a geometric rate within a system and can quickly consume space rendering a system useless.

- Worms. A worm is also an independent, self-replicating agent program that seeks to "travel" to other computers. It also grows at a geometric rate quickly spreading and infecting other systems.

- Virus A virus is a dependent self-replicating agent. It requires a host program where it will hide until executed in a "clean" system, at which time it can spread to other programs within the new system, possibly damaging them on the way. In the past few years, viruses have been designed to be significantly more crafty and lethal to systems This third generation (18) of virus is called the "Dynamic Stealth Virus" and has the capabilities to replicate its code, encrypt and decrypt itself and also mutate its encryption codes.

- Bombs A bomb is a device that is set to "explode" and can be triggered at a certain time or by a particular event. The explosion can do significant damage to the host machine.

- Trojan horse So named for its similarity to the wooden horse that was placed outside the gates at the city of Troy with its "warriors" hidden inside Once inside and past all the city's defenses, the "warriors" were free to exit the horse and execute their destructive missions. In the same way, a Trojan horse

program gains entry to "clean" systems and then through the aid of conditional tests can be left "dormant" for long periods of time until its actions are desired.

- Back doors. Called back door because normally people that use the back door of a house are family members or friends that are not required to pass through the normal security measures at the front door. This is a secret "access port" installed in a system by the attacker with the intention of using it at a future time, even during times of heightened security.

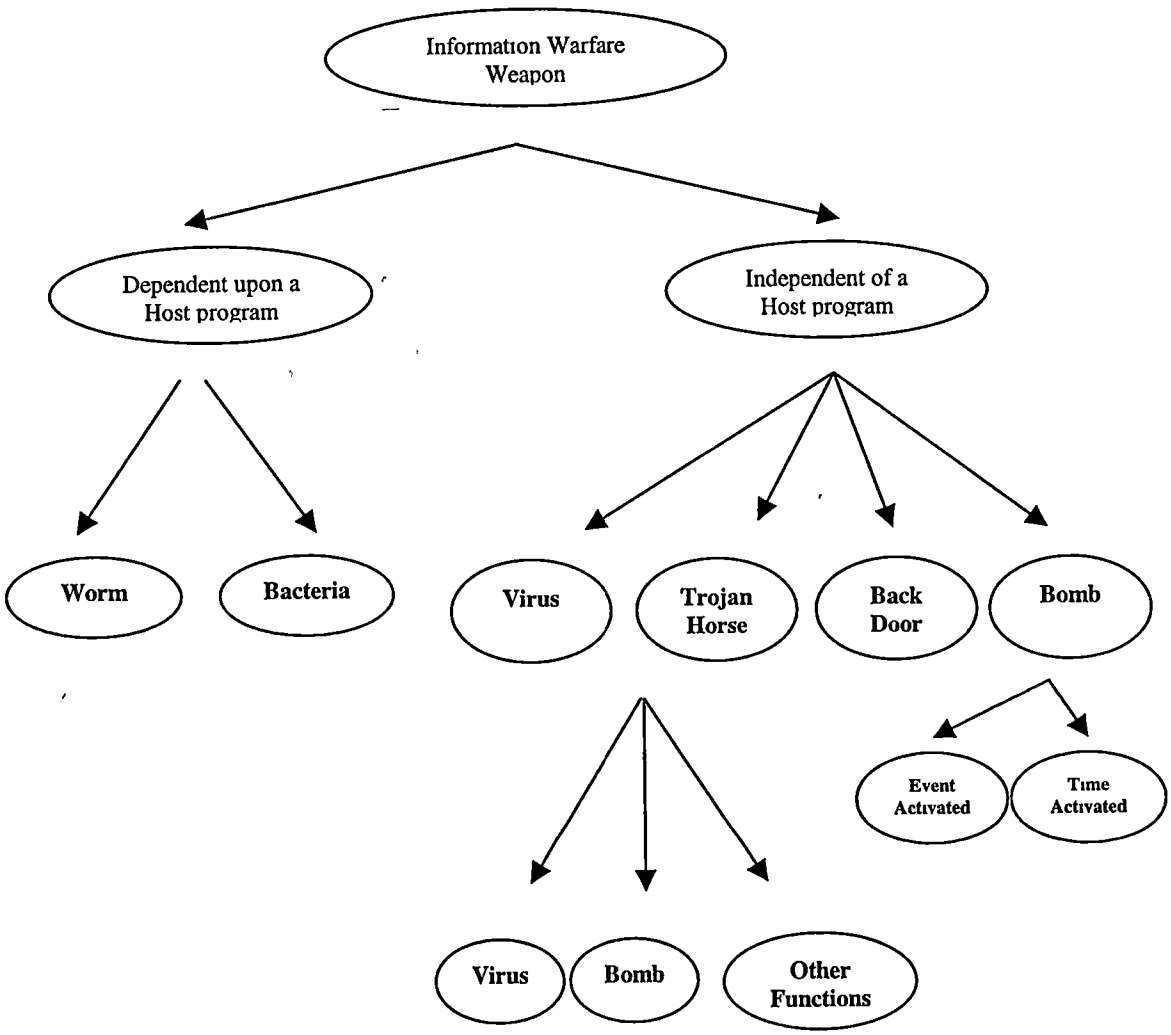

Figure 3-1. Classic Information Warfare Weapons

Offensive Information Warfare Attacks and Airliner

There are nine different fundamental disciplines, in which six of them are relevant to offensive information warfare against aircraft. Figure 3-2 is used to show where each type fits in with respect to information warfare

- Psychological Operations (PSYOPS) Planned operations to convey selected information to a foreign audience The objective is to manage the perception of the targeted population, with the agenda of encouraging the outcome in a beneficial way that favors one's cause, not necessarily that of the target's. The controlled use of the media to one's advantage can be a form of PSYOPS. The increasing use of public opinion polls in the decision process demonstrates that perception is indeed effective in the modern world. PSYOPS can be used extremely effectively against an industry or individual company in the free society where competition exists For example, the Internet could be used to start a slander campaign against a particular airline with the goal of driving the airline out of business, or at least adjusting the market distribution. PSYOPS is not new, it is just a new vehicle to continue this form of warfare that has existed for years

- Deception Deception operations are creating a false impression of reality As was utilized in Tom Clancy's book Debt of Honor, when the News networks continued to portray the US Aircraft Carriers in port at Pearl Harbor, when in reality they were at sea steaming to the Op area. Deception can be used on the Internet to lure people or companies to do things or make decisions that they might not normally make. It can be easily used to commit fraud and the Internet is a perfect vehicle for that, but it does not present any direct danger to aircraft safety

- Electronic operations It is composed of electronic warfare and network operations that concentrate on the network infrastructure. Electronic warfare has traditionally been restricted to military and this thesis will only address relevant topics, such as navigation warfare Network operations are information based and are conducted in cyber space.

    1) Navigation warfare Is a form of warfare that attacks navigation systems such as global positioning systems or radio navigation systems. The DOD's GPS satellite navigation system is fairly resistance to disruption for aircraft navigation. Most GPS receivers are only mounted

Information Warfare Model	Function	Operations
Offensive	**Perceptual**	PSYOPS and Deception
	Information	Network operations Electronic warfare Ops
	Physical	Physical destruction
Defensive	**Perceptual**	Intelligence Counterintelligence
	Information	Information security Electronic warfare Ops
	Physical	Operational security

Figure 3-2 Fundamental Disciplines of Information Warfare

on the upper surfaces of aircraft, giving them some built in signal rejection from ground based jamming signals or deception signals. Jamming a GPS signal is not technically very difficult nor extremely expensive, but since most GPSs are only used to update inertial navigation systems, locally denying an aircraft of the GPS signal will have little effect on an airliner (but could have a large impact on the military's use of precision guided weapons). Spoofing is making an aircraft's navigation systems present false positions GPS spoofing is feasible, but to date is not practical and therefore not yet a threat to airliners.

There are various radio navigation methods in use today, and all are susceptible to denial and deception by even the "low tech advisory" and during the cold war, Soviet bloc countries routinely altered these navigation signals.

2) Network operations. This is the heart of "cyberwar" and is information-based war against the infrastructure of a nation or any other entity that has become dependent on information based technology. This

thesis will thoroughly cover this topic, especially as it relates to the airline industry.

- Physical destruction. As compared to attacking information-based systems with "ones and zeros", this is physically destroying or damaging the "systems". The physical damage could be in the form of knocking out the power to the system or a direct attack with military explosive weapons. This will not be addressed in this thesis, as it is not relevant.

Conclusion of Offensive Information Warfare

The data overwhelmingly supports the theory that offensive information warfare crime is on the rise. At the same time the technology being utilized by these criminals is comparable (same level of technology) to that employed in defensive measures. The number of information systems with access to NII/GII is increasing in virtually all sectors of industrialized countries and with this comes the criminal element. If adequate resources are not allocated to protecting these systems from not only kids out for a "joy ride on the Internet", but also determined criminals, the overall utility of these large information infrastructures will be significantly reduced This could also cause public confidence to falter in this advanced information system that would, in turn, slow down progress. Defensive information warfare will be discussed in Chapter IV.

CHAPTER IV

DEFENSIVE INFORMATION WARFARE

Defensive information warfare is all measures taken in an effort to protect or defend an information system or information network from attacks from cyber-space. The term "information assurance" is the new phrase being used for defensive information warfare Moving a vital computer into a bunker deep underground can only protect it from physical attacks and will have no effect on its vulnerability to information warfare attacks. The next obvious solution might be to close all access ports of the computer to the outside world, this can also be the most ineffective solution that managers must resist the temptation to implement, as it normally drastically reduces the capability of the computer to virtually nil Alvin Toffler and his wife consider the United States in a post "industrial revolution", called the third wave or "information revolution" (24). Countries such as the United States, where computers and information systems are well established in all aspects of life, has caused these countries to become increasingly dependent upon this new technology, thereby, raising the vulnerability of these systems to new levels. In the past there were always "manual" back-ups, but now, if for example, the fly-by-wire computers in an aircraft are inoperable, the aircraft will cease to fly.

Risk management acknowledges that risk avoidance is most likely not practical and some information warfare attacks may be successful. The most effective method is to deny the

"would be attacker" access to the system; this could alleviate 80% of attacks (2). Next, detect unauthorized users on the system, which might prevent another 19% This leaves only 1% of the "would be attackers" that must be confronted. The fundamentals for computers and information systems security are as follows·

- Availability The amount of time a system is in an up status (operational), as compared to the time the system is down for maintenance or other problems. Obviously, the goal is to maximize the up time and minimize the down time in order to increase the usefulness of the machine. In this way, the probability is increased that the system will be functioning when it is required.

- Integrity. The assurance that the information and system remain secure from unauthorized intrusion or destruction. Various method may be used such as encryption, dedicated transmission methods, system monitoring by security personnel utilizing complex monitoring programs and built in alarm systems to detect "break-ins".

- Authenticity. The system should be able to identify users and then only permit access to authorized users and even further restrict access to those specific areas that are required by the specific user

- Non repudiation assures that transactions are immune from false denial of sending or receiving information, by providing reliable evidence that can be independently verified to establish proof of origin and delivery.

- Confidentiality The system should have the capacity to prevent unauthorized systems or persons collecting, observing the information or flow of information. These actions could be used to acquire unauthorized information or at least identify other nodes on the network

- Restoration. After an attack, the system should be capable to recoup and begin to operate again.

The United States government is so tremendously worried about the protection of its information infrastructure, that a new entity of the federal government has been established, which is called the National Infrastructure Protection Center (NIPC). It is located in the Federal Bureau of Investigation's (FBI) headquarters in Washington DC.

The NIPC is made up of representatives from the FBI, other federal government agencies, state and local government agencies and the private sector, all working together with the common goal of protecting this critical infrastructure. Currently, there are 60 representatives for the FBI and 40 others in the NIPC (16).

The Department of Justice and the FBI jointly established NIPC on February 26, 1998, (16). The mission of the NIPC is both national security and law enforcement, in an effort to detect, deter, assess, warn of, respond to, and then, if necessary, investigate computer intrusions and unlawful acts. Both, physical and cyber attacks that threaten and target the critical infrastructure of the United States, are considered in NIPC charter. In the Presidential directive decision (PDD) 62 and 63, signed 22 May 1998 by President Clinton, he summed up the mission of NIPC as to strengthen the Nation's defenses against terrorism and other unconventional threats to include "cyber terrorism". PDD 63 focus on the protection of the Nation's critical infrastructures from both, physical and "cyber" attacks. President Clinton's introduction to PDD 63 was:

> *"The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means for facilitating and coordinating the Federal Government's resources to an incident, mitigating attack".*
>
> William J. Clinton

In the introduction of the NIPC charter, the president outlined very well the root of the concerns by stating that the United States functions because the private sector is successful and therefore it must be adequately protected by a collaborative effort of the government and civilian sectors.

"Because so many key components of our society are operated by the private sector, we must create a genuine public/private partnership to protect America in the 21st century. Together, we can find and reduce the vulnerabilities to attack in all critical sectors "

William J. Clinton

As defined in PDD 63 (May 98) and the President's Commission on Critical Infrastructure Protection (Oct 97), the "critical infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government. These systems are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. They are broken down into the following eight general groups:

- Information and Communications. The equipment, software and processes that support the national computing and telecommunications capability

- Energy. The two major sources of energy are electricity and oil/gas. The electrical generation stations, transmission and distribution networks that generate and supply power to the end-users in order for the end-user to maintain minimum operations and the production, holding/processing facilities for natural gas, crude and refined petroleum are included in the critical infrastructure.

- Banking and financial systems. This includes retail and commercial organizations, investment institutions, exchange boards, trading houses, and the capital reserve system. Basically this encompass everything that deals with money.

- Water system. This includes the source, storage, transportation, and treatment of water for domestic and industrial uses.

- Transportation. This is the national infrastructure of all modes of transportation that support the national security and economic well being of the nation.

- Government operations. These are the minimum level of Federal, state and local levels of government which are required to meet the essential needs of the public.

- Emergency services. These include medical, police, fire and rescue systems, as well as the personnel that are required to respond to emergencies.

- Public health services. These include prevention, surveillance, laboratory services and personal health services.

All of the systems mentioned above can be considered valid military targets during conflicts, as well as always being targets of opportunity for terrorism.

In order to defend a system from information warfare attacks, the access ports could be closed, but this is not practical for the reasons stated earlier, therefore, a method of identifying authorized users and only allowing them access to the specific areas that they require, must be developed. As the last resort, a system must be capable of a rapid recovery if an information attack is not detected and repealed. The majority of digital traffic in cyberspace is propagated via the public airways or telephone lines, neither of which is considered secure or extremely resistance to unauthorized intrusion. This only supports the theory that the most effective method of defending a system against information warfare attacks, is employing software and hardware protections **contained within the systems being protected,** rather than depending on the entire system remaining secure or the use of external security.

Defending Airliners from Information Warfare Attacks

As discussed earlier, in order to protect a system from information warfare attacks, three basic principles should be employed:

- First, prevent unauthorized stations from being able to receive the transmissions, be it via telephone, hard lines, or RF transmissions.
- Second, ensure that even if the signals are received, they are not intelligible to unauthorized person/systems due to encryption.
- Thirdly, ensure that ALL message traffic over the network is first authenticated, to ensure that it is from an authorized user

The protection of airliners from information warfare attacks, while still allowing the aircraft to remain digitally connected to land based information systems, can be a challenge.

Regardless of the medium of the transmission, be it a FAA network or an airline's dedicated system, the up link to the aircraft must use electromagnetic radiation and currently the two options are a satellite link or a RF signal from a ground station directly to the aircraft. These two methods were discussed earlier in Chapter II, but now they will be addressed from the security point of view.

Between fixed locations, it would be relatively easy to protect a data link signal from possible intrusion by employing highly directional antennas, thereby reducing the "footprint" of the signal to include only the authorized stations. For obvious reasons, this is not even relevant, as airliners are neither fixed nor predictable platforms with respect to

communications. The United States military has tried many different methods in order to ensure secure aircraft communication over the years and has never found one totally secure and reliable method. Some of the difficulties encountered in making secure digital communication between a ground station and an aircraft are:

- The majority of aircraft are not at a fixed location.
- Airliners must have the ability to communicate with multiple different stations simultaneously.
- The wide variety of type of aircraft that must be connected to the "net", such as airliner, military aircraft, helicopters, light civilian, etc.

To determine if a secure and reliable method of digitally communicating with aircraft exists, all aspects of the signals must be considered from the point of view of security and reliability. The terms "critical" and "vital" may be used in different contexts to have very different meanings. From the standpoint of an airline company, the navigation and environmental control computer (that regulates the temperature) are vital and critical to mission accomplishment. To airworthiness, the fly-by-wire computer is vital and critical to flight. Some considerations and techniques in the search for a secure and reliable method of digitally security while communicating with aircraft are:

- The communication methods such as the Internet, telephone lines or RF signals are extremely vulnerable to intrusions, i.e., information warfare attacks, and should be used only if the signal is **encoded.**
- Whenever a RF link is used, directional antennas should be used whenever possible. Emerging new technology in electronically focused antennas may make this possible to employ directional antennas with moving aircraft.

- Communications via satellite offers the most inherently secure method of communications for aircraft with respect to information warfare. The aircraft antennas can be oriented up, thereby significantly reducing the sensitivity to signals originating from the surface. This, in effect, would reduce the risk of deceptive signal being received from surface transmitters.

- The software programs at all levels should incorporate routines to authenticate and verify the identity of every station before access is granted. This must also be done before any information is accepted from another station. Even once the identity of the sender is verified, a state of the art software program should be used to ensure that the incoming message/program is not a carrier of a dangerous sub-routine or sub-program hidden in the coding such as a virus or a worm.

- Each user of a system must be granted access only on a need to know basis and DO NOT MAKE global access the norm, but rather the exception.

- Ensure that vital systems, if possible, are separated from other systems that are connected to the external "world", for example, the flight control computer of an airliner is totally independent from the mission computer, which could be connected to the FAA and also the flight dispatcher. By doing this, if one system is incapacitated by an information warfare attack, the critical function such as flight controls remain functioning.

- When vital systems must have access to the external world, a "firewall" should be installed. This is where a computer is used between the critical system and the outside world to act as a buffer. This is one of the simplest and cheapest forms of protection to reduce the probability that any undesired "bugs" are granted access.

- If jamming becomes a threat, frequency agile radio should be used to reduce the effects of jamming. The military has for years been employing frequency-hopping radios, which frequency hops at a rate in the order of 10 channels per second. These techniques are used to help protect the signal from unauthorized access and to reduce the effects of jamming.

Conclusion on Defensive Information Warfare

Without taking drastic measures that might also render an information system useless (such as completely closing all access ports to include the disk drives), the risk of the system being attacked by cyber warriors CAN NOT BE TOTALLY AVOIDED. Therefore, the risk of information warfare attacks should be managed by employing the following three concepts:

- Accept risk. Unless the protective measures are far more sophisticated and robust than the capability of the threat, some degree of risk must be tolerated and accepted.

- Mitigate risk. Do not allow different subsystems to have "global" access. In this way, when one sub-system is compromised (penetrated), the entire system is not lost. An example of this is not to allow the same computer that handles digital information from external sources to have ANY access to the flight control computer or engine control computers.

- Avoid risk. Ensure that security measures are layered to ensure that the "inter-core" of the systems (the most important area), is under the highest level of security. The flight control computer of a *fly-by-wire* aircraft must be protected from attacks at **ALL COSTS** and if it can not be adequately protected it should be removed or a manual back-up installed. Therefore these critical computers should not have any sensors (information/data ports) external to the aircraft directly connected to them.

As this chapter has demonstrated, there are currently available methods for reducing the susceptibility of intrusion into information systems and data links by unauthorized persons. As the airline industry and the FAA move further down this slippery road towards digitally integrating airliner with the ground based communication infrastructure, great care must be taken to always employ the state of the art security equipment. The

possible risk to human lives would be excessive if an airliner's critical onboard computer were vulnerable to incapacitating information warfare attacks

CHAPTER V

CONCLUSION

The purpose of this thesis was to determine if modern aircraft are currently at risk of falling victim to information warfare attacks or if they could be in the near future (less than 10 years). If they were determined to be at risk, protective measures would be discussed and evaluated for effectiveness and specific suggestions will be made as to their value.

It is hoped that the reader of this thesis now fully appreciates the threat to digital communications and the information infrastructure in the United States and Globally from information warfare attacks The reality is that these attacks can and are being successfully executed at an extreme cost and/or danger to the ill prepared.

Where human lives are on the line, as well as the outcome of battles, the military, even using the utmost care to prevent unauthorized intrusions, still falls victim to information warfare attacks. The banking and finance industries, that exists solely to properly manage money, employs the most skillful experts (some even being ex-hackers), with the "latest and greatest" techniques to protect the integrity, while **allowing access by authorized users or clients, STILL FALLS VICTIM OF COSTLY INFORMATION WARFARE ATTACKS.** This demonstrates that "industry/government" are possibly expending too little time and assets on advancing defensive information warfare measures.

It must be noted that, to date, neither the airline industry nor the FAA has experienced large-scale attacks by cyber warriors, even though the industry is becoming more susceptible to such attacks. This absence of attacks SHOULD NOT BE used to lull oneself into a false sense of security with the conclusion that the industry is properly protected from information warfare attacks. The explanation is most likely that, to date, the lions share of attacks have been conducted against industries that offer a financial reward or a challenge to the attacker, such as the military. Today some industries have been spared from these disabilitating attacks, not due to adequate protective measures, but rather luck or not being lucrative targets. The military does not enjoy this "protection" and is being hit daily by information attacks, most of which are being launched by "hackers" with the only goal of seeing if they can hack into *SECRET* areas.

It should be understood that most network systems in the future will be connected to an Internet type network, so as to reap the huge benefits and at the same time, they also expose themselves to the increased risk of being attacked. As a general rule, the benefits of being "connected" to the world far out weigh the risks associated with it. Therefore, private industry and governments should implement the state of the art protection in multi layer AND also prepare to be penetrated. There are currently methods available for reducing the susceptibility of unauthorized intrusion, they are expensive but MUST be implemented in order to protect the information system

BIBLIOGRAPHY

BIBLIOGRAPHY

Adams, James, 1998, The Next World War, Simon and Schuster, New York, NY.

Associated Press, 01 April 1999, "Computer vaccine industry growing", In The Stars and Stripes (US military forces overseas daily newspaper).

Computer Security Institute, 05 March 1999, 1999 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, San Francisco, CA.

Denning, Dorothy E., 1999, Information Warfare and Security, Addison Wesley Longman, Inc., Reading, MA.

William S. Cohen (Secretary of Defense), May 1997, Quadrennial Defense Review, Department of Defense, (available on the internet at http://www.defenselink mil/ pubs/qdr/)

Gay, Martin and Gay, Kathlyn, 1996, The Information Superhighway, Twenty-First Century Books, New York, NY.

Government Administration Office, 22 May 1996, AIMD 96-84/92 (Information Security Computer Attacks at DOD Pose Increasing Risks), http://www. gao.gov/AindexFY96/ abstracts/ai96092t html

Hills, Wes (Cox News Service), 12 April 1999, "Hacker slips into Air Force critical weapons database", The Stars and Stripes (US military forces overseas daily newspaper)

Johnson, Chris, 1997, Jane's Military Avionics, 1997-1998, Jane's Information Group Limited, Surrey, UK.

Joint Chiefs of Staff, 1998, Joint Vision 2010, Department of Defense, Washington DC.

Kornblum, Janet, 01 April 1999, "Digital hunt on for e-mail virus-maker", USA Today

Molander, Roger, Riddile, Andrew and Wilson, Peter, 1996, Strategic Information Warfare, A New Face of War, RAND, Santa Monica, CA.

National Infrastructure Protection Center, downloaded 01 September 1999, URL http:/www fbi/nipc/home.html, Washington DC.

Naval Air Warfare Center, 1993, Electronic Warfare and Radar Systems Engineering Handbook, Naval Air Systems Command (AIR-546), Point Mugu, CA.

Sanderson, Ward, 30 Mar 1999, "Smart ships way of the future", The Stars and Stripes (US military forces overseas daily newspaper).

Signal Magazine, 1996, Information Warfare Series, Computer Sciences Corp., Falls Church, VA.

Seffers, George, 08 March 1999, "DOD may seek tech boost", Defense News.

Tanenbaum, Andrew, 1991, Redes de Ordenadores (Computer Networks), Prentice-Hall Hispanoamericana S.A , Englewood Cliffs, Mexico

Toffler, Alvin, 1991, The Third Wave, Mass Market Paperback.

Under Secretary of Defense for Acquisition, Transcription of the 1995 Conference on COTS, COTS 95 Conference, http //www.mc com/cots_folder/cots95/cots95_toc.html.

United States Army, 27 August 1996, FM 100-6 (Information Operations), United States Army.

United States Marine Corps, 02 June 1999, MCRP 6-22C (Radio Operator's Handbook), United States Marine Corps.

Waltz, Edward, 1998, Information Warfare Principles and Operations, Artech House Inc , Norwood, MA.

Williamson, John, 1997, Jane's Military Communications, 1997-1998, Jane's information Group Limited, Surrey, UK

LIST OF REFERENCES

LIST OF REFERENCES

1. Gay, Martin and Gay, Kathryn, "The Information Superhighway", Twenty-First Century Books, New York, NY, 1996

2. Denning, Dorothy E., "Information Warfare and Security", Addison Wesley Longman, Inc , Reading, MA, 1999.

3. Signal Magazine, "Information Warfare Series", Computer Sciences Corp., Falls Church, VA, 1996.

4. Molander, Roger; Riddile, Andrew and Wilson, Peter, "Strategic Information Warfare, A New Face of War", RAND, Santa Monica, CA, 1996.

5 Adams, James, "The Next World War", Simon and Schuster, New York, NY, 1998

6. Tanenbaum, Andrew, "Redes de Ordenadores" (Computer Networks), Prentice-Hall Hispanoamericana S A , Englewood Cliffs, Mexico, 1991.

7. Naval Air Warfare Center, "Electronic Warfare and Radar Systems Engineering Handbook", Naval Air Systems Command (AIR-546), Point Mugu, CA, 1993.

8. Williamson, John, "Jane's Military Communications, 1997-1998", Jane's Information Group Limited, Surrey, UK, 1997.

9 Chris, Johnson, "Jane's Military Avionics, 1997-1998", Jane's Information Group Limited, Surrey, UK, 1997.

10. Eisler, Peter, "Security at 2 weapons labs called marginal", USA Today, 01 April 1999.

11. Elmore, Cindy, "Melissa swamps military system", The Stars and Stripes (US military forces overseas daily newspaper), 30 March 1999

12 Hill, Wes (Cox News Service), "Hacker slips into Air Force critical weapons database", The Stars and Stripes (US military forces overseas daily newspaper), 12 April 1999.

13. Associated Press, "Computer vaccine industry growing", The Stars and Stripes (US military forces overseas daily newspaper) 01 April 1999.

14. Seffers, George, "DOD may seek tech boost", Defense News, 08 March 1999

15. Valenzuela, Javier, "The web of Chinese espionage", El Pais (One of Spain's daily newspapers), 31 May 1999

16 National Infrastructure Protection Center, "http /www fbi/nipc/home html", Washington DC, downloaded 01 September 1999.

17 United States Army, "FM 100-6" (Information Operations), United States Army, 27 August 1996

18. Waltz, Edward, "Information Warfare Principles and Operations", Artech House Inc , Norwood, MA, 1998

19. Joint Chiefs of Staff, "Joint Vision 2010", Department of Defense, Washington DC, 1997.

20. Computer Security Institute, "1999 CSI/FBI Computer Crime and Security Survey", Computer Security Institute, San Francisco, CA, 05 March 1999

21. United States Marine Corps, "MCRP 6-22C" (Radio Operator's Handbook), United States Marine Corps, 02 June 1999.

22. Under Secretary of Defense for Acquisition, "COTS 95 Conference", http://www.mc.com/cots_folder/cots95/cots95_toc.htms, Transcription of the 1995 Conference on COTS

Government Administration Office, "AIMD 96-84/92" (Information Security. Computer Attacks at DOD Pose Increasing Risks), http://www.gao.gov/AindexFY96/ abstracts/ai96092t html 22 May 1996

24 Toffler, Alvin, "The Third Wave", Mass Market Paperback, 1991.

APPENDICES

APPENDIX A

YAHOO SEARCH. KEY WORD "INFORMATION WARFARE"
(08 DEC. 99)
(The bolded item will be appendix B)

Yahoo! Site Matches (1 - 19 of 41)

Government > Intelligence > Information Warfare

RST Information Warfare
Information Warfare Questing Power Via Cyberspace - explores the information warfare mania
Information Warfare Database - searchable database of information warfare attacks and computer crimes that have occurred in the past 15 years
Information Warfare/InfoSec
Glossary of Information Warfare Terms
Institute for the Advanced Study of Information Warfare
Introduction to Information Warfare
Information Warfare - Defense
Web Directory Information Warfare Resources
Information Warfare Documents
Information Warfare on the Web - extensive resources from the Federation of American Scientists
Information Warfare Research Center
Information Warfare-Protect Systems Engineering Division

Social Science > Science, Technology, and Society

Technological Warfare - information regarding technological warfare, information warfare, and computers implementation for military purposes

Arts > Humanities > History > By Time Period > 20th Century > Military History > World War I > Chemical Warfare

Death on the Wind Gas Warfare - includes pictures and information on the hazards of gas warfare in WW1

Arts > Humanities > History > By Subject > Military History

Ancient Warfare - essays and information ancient history, and links to primary source sites

Government > Military > Weapons and Equipment > Chemical and Biological

Chemical and Biological Defense Information Analysis Center - serves as the focal point for chemical warfare and biological defense technology

Government > U S Government > Executive Branch > Departments and Agencies > Department of Defense > Defense Technical Information Center - DTIC

Chemical and Biological Defense Information Analysis Center - serves as the focal point for chemical warfare and biological defense technology

APPENDIX B

INSTITUTE FOR THE ADVANCED STUDY OF INFORMATION WARFARE (IASIW)

(bolded item will be appendix C, "Cyberterrorism· RAND Corporation report")

Information warfare, also known as I-War, IW, C4I, or Cyberwar, has recently become of increasing importance to the military, the intelligence community, and the business world The purpose of the IASIW is to facilitate an understanding of information warfare with reference to both military and civilian life

"Communications without intelligence is noise, intelligence without communications is irrelevant "
Gen Alfred M Gray, USMC

" attaining one hundred victories in one hundred battles is not the pinnacle of excellence Subjugating the enemy's army without fighting is the true pinnacle of excellence "
Sun Tzu, The Art of War

This page will help you increase your understanding of information warfare For those unfamiliar with the term, "Information Warfare" the following definition may be helpful

Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own Such actions are designed to achieve advantages over military or business adversaries
Dr Ivan Goldberg

Glossary of information warfare terms

2600 The Hacker Quarterly
Abstracts of articles on protecting computer networks
ACLU to spy on Echelon (Oakes)
Advanced Technology Demonstration Network (ADTnet)
Air Force Computer Emergency Response Team (AFCERT)
Air Force Information Warfare Center
Alerts from the NIPC
Anonymous communication on the Internet.
Army dumps Microsoft, adopts Apple to avoid hackers (Glave)
Back Orifice A security alert advisory
Banks appease online terrorists (Shelton)
The battlefield of the future 21st century warfare issues
Bibliography of readings on IW (Shope)
Another bibliography on IW (Sanz)
Big brother covets the Internet (Brandt)

Big brother in cyberspace
Books on Computer Crime
Books on Computer Security
Books on Computer Viruses
Books on hacking
Books on Information Warfare
Books on Internet Security
Books on TCP/IP
Books on Telecommunication Networks
British government site devoted to communications-electronics security
Buffer overflow attacks (Rothke)
Bugging Types of technical surveillance devices
Bulgaria and computer viruses (Bennahum)
Business and IW (Alvarez)
C2 Bibliography
CALEA Communications Assistance for Law Enforcement Act
CALEA Communications Assistance for Law Enforcement Act---Text of the act
Canadian government report on Information Operations
Canadian government site devoted to information technology security
Canadian information operations (Bourque)
Center for Secure Information Systems (CSIS)
A Chinese view of information warfare (Mengxiong)
Another Chinese view of IW
The CIA and information warfare (Elliston)
CIAC Bulletins
CIPHER Electronic newsletter of the technical committee on privacy and security of the IEEE
Class III information warfare has it begun? (Schwartau)
Common criteria for information technology security
Computer attacks utilizing large data packets (Hannaford)
Computer crime bibliography (Anderson)
Computer crime categories (Carter)
Computer crime The Department of Justice perspective
Computer crime An historical survey (Overill)
Computer crime An introduction (Fraser)
Computer crime laws by state
Computer crime prevention
Computer crime sentencing guidelines (King)
Computer crime statistics (Kabay)
Computer crime. What it costs
Computer Emergency Response Team (CERT)
Computer espionage (Defense Investigate Service)
Computer fraud
Computer Security Day
Computer security F A Q s
Computer security information
Computer security, law, and privacy
Computer virus library
Computer virus myths (Rosenberger)
Computer virus warnings, How to tell the real from the hoaxes (Ford)
Computer viruses in information warfare (Cramer & Pratt)
Congressional testimony by the CIA on information warfare
Considering the Net as an intelligence tool (Wilson)
Cornerstones of information warfare (Fogleman & Widnall)

DoD's vulnerability to information warfare (Levin)
Dominant battlespace knowledge (Johnson & Libicki)
ECHELON and other interception capabilities (Campbell)
ECHELON. A global surveillance network. (Verton)
ECHELON New Zealand's involvement (Hager)
Economic/industrial espionage. (Venzke)
Economic espionage. An information warfare perspective (Cramer)
Economic espionage, technology transfers and national security (Saxton et al.)
The economic impact of IW (Saarelainen)
Electromagnetic and electronic systems U S / Navy site
Electromagnetic evesdropping
Electromagnetic hazards ()
Electromagnetic radiation and the brain A bibliography (Beck & Byrd)
Electromagnetic environmental effects Electromagnetic weapons of mass destruction (Kopp)
Electronic civil disobedience (Wray)
An electronic Pearl Harbor? Not likely (Smith)
    More on electronic Pearl Harbor
Eligible receiver. (Gertz)
More about Eligible receiver
Email and espionage
Email security problem
Email Which free services are secure?
Emission security assessments
Emission security countermeasures
EMP/T bombs
EMP and TEMPEST hardening U S. Army document
Encryption in crime and terrorism (Denning & Baugh)
Encryption. Why the government cannot control civilian use (Forno)
Errors that lead to computer security vulnerabilities.
E-strikes and cyber-sabotage Civilian hackers go online to fight (Riley)
The ethics of civil defense and information warfare (Schwartau)
The ethics of information warfare (Kuehl)
European Union directive on data protection
The FBI's domestic counterterrorism program
The FBI and electronic surveillance
The FBI and email
The FBI's infrastructure protection and computer intrusion squad
Federal Communications Law Journal
Federal computer surveillance
Federal Intrusion Detection Network (FIDNET) (Frank)
FIDNET. Civil liberties concerns.
Fighting computer viruses (Kephart et al)
Fighting Internet crime (Lash)
Financial information networks Protecting them from intrusion (Stolfo)
Financial information networks Vulnerability to hackers (Winkler)
Firewalls. (Robinson)
Firewalls---How to select one.
    Foes with grudge sludge Drudge (Glave)
Forecasting model for Internet security attacks (Korzyk & VanDyke)
France changes policy regarding cryptography (Oram)
A French IW site
A function model of information warfare (Johnson)
Fundamentals of information warfare---An airman's view (Foglerman)

The future of information security (Libicki)
GAO on DoD INFOSEC
Generally-Accepted System Security Principles (GASSP)
German government site devoted to information technology security [in Genman]
Global information security (Libicki)
Governmental (USA) electronic surveillance activity
The great cyberwar of 2002 (Arquilla)
Guerrilla warfare in cyberspace
HAARP Highfrequency Active Auroral Research Project
Hacked Web pages An archive
Hacked Web pages Another archive
Hacker's ethics
Hacker sentenced to prison Press release of the Department of Justice
Hacker wargames
Hacker's view of hacking
Hackers How should we respond? (Ludlow)
Hackers penetrate DoD computer systems
The hacker's mind set (Rist)
Hackers who break into computer systems (Denning)
Hacking in 1999
    Hacking Nasdaq (Oakes & Kahney)
Hacking the power grid (Koprowski)
Hacking TCP/IP (Shimomura)
Hacking U S Government Web sites (Mueller)
Hacking the Web (McNamara)
Hardwar, softwar wetwar operational objectives of information warfare (Wilson)
The heads and tails of information (Baklarz)
Hearing on current and projected national security threats (Tenet)
HERF (High Energy Radio Frequency) weapons
HERF An FAA course
HERF gun proliferation
HERF and the Panama Canal
Higher education and information security (Reynolds)
Hotmail security problems
Human intelligence and covert action
    Identity theft (Hayes)
IE 5 security bug (Louderback)
Improving the security of your site by breaking into it (Farmer)
Induced fragility in information age warfare (Fowler & Peterson)
Industrial espionage Who's stealing your information (Denning)
The information age Its impact and consequences (Alberts & Papp)
Information assurance and the information society (Luijf)
Information insecurity (Peters)
Information operations
Information operations Applying the principles of war (Nelson)
Information operations, deterrence, and the use of force (Barnett)
Information operations in Bosnia A preliminary assessment (Allard)
Information operations and information systems (Tulak & Hutton)
Information peacekeeping (Steele)
Information risk management (Byrnes)
Information security Implementing policy (Wood)
Information, technology, and the center of gravity (Harley)
Information war and the Air Force Wave of the future or current fad? (Buchan)

Information warfare in 2025. (Stein)
Information warfare The possibility of disaster. (Carver)
Information warfare and the U S Marine Corps (Yeary)
Information warfare defense (Defense Science Board)
Information security· Computer attacks on Department of Defense pose increasing risks
Infowar (Browning)
Information warfare (Lewis)
Information warfare in the business world (Winkler)
Information warfare Defeating the enemy before battle (Ivefors)
Information warfare and deterrence (Wheatley & Hayes)
Information warfare Developing a conceptual framework (Garigue)
Information warfare with electromagnetic attack
Information warfare and information security on the Web.
Information warfare is not InfoSec repackaged (Schwartau)
Information warfare in international law (Greenberg et al)
Information warfare· Issues and perspectives (Miller)
The information warfare mania (Whitaker)
Information warfare. The perfect terrorist weapon (Shahar)
Information warfare A philosophical and sociological perspective (Bey)
Information Warfare Planning the Campaign (Ayers, et al)
Information warfare and security. A slide show (Denning)
Information warfare weapons
Inforsec. What is really important (Forno)
From InfoWar to knowledge warfare (Baumard)
Infrastructure protection (Schwartau)
Infrastructure protection and threats to civil liberties (O'Neil & Dempsey)
Infrastructural warfare An introduction
Infrastructural warfare slides (Wilson)
Intelligence agencies of the world - - - listed by country.
Intelligence-based threat assessments for information networks and infrastructures (Anderson)
Internet and cyber-terrorism (White)
Internet firewalls An FAQ (Ranum et al)
Internet security
Internet Security Handbook (U S Navy)
International controls over information warfare (Verton)
International computer intrusions (Anderson)
International electronic surveillance by the USA. Civil liberties aspects (ACLU et al)
International legal implications of information warfare (Aldrich)
Internet as an intelligence tool (Wilson)
INTERNIC security hole
An introduction to information warfare (Haeni)
Intrusion detection An FAQ
Intrusion detection.
Intrusion detection New methods (Cramer et al)
The IW threat from sub-state groups An interdisciplinary approach (Rathmell et al.)
IP spoofing demystified
More about IP-spoofing
Joint force superiority in the information age (Paige)
Joint Military Intelligence College (JMIC)
Journal of Electronic Defense
Journal of Intrastructural warfare
Journal of Internet Security
Keeping information warfare in perspective. Gompert)

Knowledge strategies Balancing ends, ways, and means in the information age (Fast)
KUBARK How the CIA obtains information
Legal aspects of cyberspace
The Maginot line of information systems security (Forno)
The mesh and the net Speculations on armed conflict in an era of free silicone (Libicki)
Microsoft vs hackers (Shankland)
Microsoft and security Mutually exclusive terms (Forno)
Military information operations in a conventional warfare environment
MKULTRA Another type of information warfare (Elliston)
MKULTRA Senate report
Mobilization for a new era (Wik)
MS Office leaks sensitive data (Oakes)
National Cryptologic Museum
National cryptologic strategy for the 21st century (NSA)
National Infrastructure Protection Center (NIPC)
Federal photoidentity database. (McCullah)
The National Security Agency (NSA)
More information about the NSA
NSA offers INFOSEC courses
National security in the information age (Devost)
Navy INFOSEC website
The NSA Handbook
Navy INFOSEC Web site
Network Centric Warfare. (Stein)
More on Network Centric Warfare (Brewin)
Network Centric Warfare. Seven deadly sins (Barnett)
NT Web technology vulnerabilities (rain forest puppy)
OASD C3I
Online privacy A guide (Center for Democracy and Technology)
Pentagon's computers vulnerable to hired hackers (Myers)
Pentagon cybertroops The national security apparatus gears up for infowar (Overbeck)
Pentagon vs hackers (Miklaszewski & Windrem)
Piercing firewalls
Political aspects of class III information warfare Global conflict and terrorism (Devost)
The political demographics of cyberspace
Precautionary disconnects form the Internet. (Rosenberger)
Psychotronic Weapons Myth or Reality? (Pavlychev)
Radio frequency weapons Congressional testimony
Radio frequency weapons (Schweitzer)
More about radio frequency weapons (Schweitzer)
Reducing cyber-threats (Revah)
Reflections on the 1997 Commission on Critical Infrastructure Protection (PCCIP) Report (Staten)
Remote viewing· The CIA's involvement with a weird version of IW (Elliston)
Report a computer intrusion or computer crime to the FBI
A revolution in military affairs (RMA) (Thomas)
More on RMA (Whitaker)
Risk assessment of the electric power industry (NSTAC)
Risk management (Meritt)
School for Information Warfare and Strategy (IWS)
Security analyzer Download one to check the security of your system
Security breaches· Examples from the media
SIGINT and the Cuban missile crisis (NSA)
The silicone spear As assessment of information based warfare (Everett et al)

Simulating cyber attacks, defenses, and consequences
SPAWAR Space and Naval Warfare Systems Command.
Strategic information warfare. (Molander)
Strategic war . in cyberspace (Molander et al)
Search for IW and Computer books
Searches and the Internet. A Canadian perspective (Hourihan)
Surveillance technology and risk of abuse of economic information
A Swedish perspective on IW
CP/IP security
TCP SYN Flooding and IP Spoofing Attacks
The technologies of political and economic control (STOA)
Telecommunications Act of 1996
Telecommunications Act of 1996 Impact on schools and libraries
\T/TCP vulnerabilities.
TEMPEST Lots of unofficial information. (McNamara)
TEMPEST monitoring.
TEMPEST in the Navy.
TEMPEST: The physics on which it is based
Terrorists and cyberspace (White)
Terrorism by email.(Szucs)
Terrorism on the Net
Terrorism and information warfare (Wilson)
Terrorism at the touch of a keyboard (Pasternak & Auster)
The third wave, What the Tofflers never told you (Czerwinski)
Threat assessments for information networks (Anderson)
Tools to increase computer security
Trojan horse attempts to gather information on Web sites (Dugan)
Trojans removal database
Truth is the first casualty of cyberwar (Smith)
Types of information warfare (Libicki)
The unintended consequences of information age technologies (Alberts)
United Nations manual on the prevention and control of computer-related crime
U. S Army Special Operations and PSYOPS
U S. cryptography policy.
U S foes targeting American computer networks (Pietrucha)
The U S intelligence community.
U S sitting duck, DOD panel predicts (Brewin & Harreld)
Uses and misuses of intelligence (Kober)
USS Liberty
The VENONA project.
Virus creation labs
Vulnerabilities of the national information infrastructure (Miller)
More on the vulnerability of the National information infrastructure (Ware)
Still more on vulnerabilities (Forno)
Waging IWar. (Wilson)
Wars of the near future (Sundarji)
Weather site penetrated by hackers. (Boyle)
What hackers know about you
What is information warfare? (Libicki)
Whitehouse report on online privacy and security (Cohen, Reno, Lew Daley)
Windows NT Trojan horse (Clark)
Windows security problem (Wilcox)
WWW Security FAQ (Stein)

Y2K hysteria A dramatic example (North)
Y2K technology problems (Koskinen)
Y2K violence
Y2K and the possibility of a cyber-attack
Created by Dr Ivan Goldberg Psydoc@PsyCom Net
Last revised 26 November 1999

There have been 097649 visitors to this page since 1 January 1996

Disclaimer

This web site is provided as a public service to increase public and professional access to timely, accurate and comprehensive information about information warfare and information security issues Considerable effort has been taken to ensure the accuracy of the information contained in this site However, no assurance is given that the information supplied is accurate or complete Links are to external resources on the World Wide Web and herefore, there is no control of the content of such information and no legal responsibility or liability for any aspect of such information is accepted or implied

>>>>>>>><!>>>>>>!>>>>

APPENDIX C

CYBERTERRORISM: RAND CORPORATION REPORT
(Bolded items are HTML links to other web pages i.e. the entire book is online)

Contents

VITA

Gregory E. Hauser was born in Orinda, California, on 30 March 1961 He attended elementary school in the Orinda School District and graduated from Miramonte High School in June, 1979. The following September he entered the University of California at Santa Barbara and in June, 1983, received a degree of Bachelor of Science in Electrical Engineering. That same month he was commissioned as a Second Lieutenant in the United States Marine Corps and reported to The Basic School in Quantico, Virginia, for six months of training Upon completion he reported to Pensacola, Florida, for basic flight training and received his wings in December 1985 He has spent twelve years flying the AV-8B and has been stationed in North Carolina, Arizona, California, Japan and Spain, four years of which were spent at China Lake, California, the United States Navy's Research/Development and Test/Evaluation base for aviation. In August 1998 he was assigned to attend the Spanish Navy's War College in Madrid, Spain

He is presently serving at the United States Embassy in Madrid as a military liaison Officer to Spain.