1-1-2003

The creation of a national information policy combating cyber terrorism

Daniel A Nick
University of Nevada, Las Vegas

THE CREATION OF A NATIONAL INFORMATION POLICY

COMBATING CYBER TERRORISM

by

Daniel A. Nick

Bachelor of Arts
Gannon University
1998

thesis submitted in partial fulfillment
of the requirements for the

Master of Arts in Ethics and Policy Studies
Institute for Ethics & Policy Studies
College of Liberal Arts

Graduate College
University of Nevada, Las Vegas
December 2002

UNLV
UNIVERSITY OF NEVADA LAS VEGAS

Thesis Approval

The Graduate College
University of Nevada, Las Vegas

April 8, 2003

The Thesis prepared by

Daniel A. Nick

Entitled

The Creation of a National Information Policy

Combating Cyber Terrorism

is approved in partial fulfillment of the requirements for the degree of

Master of Arts Ethics and Policy Studies

Examination Committee Chair

Dean of the Graduate College

Examination Committee Member

Examination Committee Member

Graduate College Faculty Representative

ABSTRACT

The Creation of a National Information Policy Combating Cyber Terrorism

by

Daniel A. Nick

Dr. Alan Zundel, Examination Committee Chair
Professor of Ethics and Policy Studies
University of Nevada, Las Vegas

The infrastructures of the United States are dependent upon computers. This creates a new threat to the national security of the United States in the form of cyber terrorism.

Cyber terrorism is the new type of warfare. It can take a cyber terrorist seconds to break into a computer network, download information, and leave without a trace. There needs to be a comprehensive policy to combat the cyber terrorism threat.

The National Information Policy is a set of ideas brought together to combat the threat of a cyber terrorist attack against the infrastructures of the United States. These ideas include: redefining the role of the military, cooperation between public and private sectors, creation of information conditions, and the establishment of a cyber court.

TABLE OF CONTENTS

ABSTRACT iii

CHAPTER 1 INTRODUCTION 1
Internet Usage Worldwide 3
Concept of Cyber Terrorism vs. Traditional Terrorism 5
Summary of Chapters 7

CHAPTER 2 PRINCIPLES OF COMPUTER SECURITY 10
History of Hacking 10
Psychological Makeup of a Cyber Terrorist 13
Psychological Makeup of a Terrorist 16
Psychological Summary 17
Information Warfare Principles 17
Defensive Information Warfare 18
Outline of an Information Warfare Campaign 21
Chapter 2 Summary 26

CHAPTER 3 CURRENT POLICIES ON COMPUTER SECURITY 28
Section I: Cyber Security Plan 28
Section II: An Analysis of the Cyber Security Plan 37
The Patriot Act 41
Chapter 3 Summary 44

CHAPTER 4 NATIONAL INFORMATION POLICY 46
Role of the Military 46
Cyberspace Boundaries 49
Information Conditions 49
Civilian Law Enforcement 51
Establishment of a Cyber Court 56
Response to a Cyber Terrorist Attack 57
Chapter 4 Summary 63

CHAPTER 5 CONCLUSION 64

ENDNOTES 66

APPENDIX I NOTIFICATION LETTER TO NICHOLAS CHANTLER 73

APPENDIX II NOTIFICATION LETTER TO DOROTHY DENNING 74

BIBLIOGRAPHY 75

VITA 78

CHAPTER 1

INTRODUCTION

The purpose of this thesis is to persuade the reader that cyber terrorism is a threat to the national security of the United States and why there needs to be a comprehensive policy on how to deal with the threat.

The dependence upon computers by the infrastructures in the United States shows how vulnerable society is to an attack. In 1996 the Committee on Protecting the Nation's Infrastructures issued a report to then President Bill Clinton that lists six infrastructures that are critical to the security of the United States. (Table 1) The committee's conclusion states that if these critical infrastructures were the victim of a cyber attack the result would be high financial losses, communication failures, and the overall inability to perform the daily functions of society. One can only conclude that if this scenario occurs there would be unrest in society.[1]

Since the committee released its findings in 1996 the government has done little to secure the nation's computer systems from a possible attack. In fact the government has received an overall grade of "F" on computer security with only the National Science Foundation scoring higher then a "C."[2] Even the recent "National Strategy to Secure Cyberspace" and the Patriot Act have limitations

and are not accepted by most in the public and private sector (as shown in chapter 4).

The policy that I have formulated is called the National Information Policy. It is not a detailed report but an outline as to the first steps the government should take to secure the nation's computer systems. I believe any computer policy, must adapt to technology and change with the makeup of society. By creating an outline, I will lay the foundation for the national computer policy for the prevention of a cyber terrorist attack. With this outline one can build upon my initial policy to create a policy in conjunction with change in technology and cyber terrorist threats.

Table 1: Listing of Vulnerable Infrastructures

	Potential Target
Food/Health	Water treatment plants water disposal plants
Energy and Communications	Public-switched facilities Pressurized natural gas pipeline systems Electric power utilities Fuel supply systems (oil, coal, etc.)
Money/Financial	IRS systems Medicare systems Federal reserve system Inter-bank systems Social Security service systems Veterans Affairs service systems Welfare systems
Transportation	Next generation of traffic control systems Public highway traffic control systems
Emergency Services/Public Safety	Law enforcement records systems Law enforcement communication FEMA systems

Source: "The Clinton Administration Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," (May 22, 1998, accessed 23 November 2002); available from http://www.nipc.gov/about/pdd63.htm; Internet.

Internet Usage Worldwide

By 1996, approximately 28 million people used the Internet.[3] In 1999, the figure more than doubled to 171 million users.[4] In 2000, the figure more than doubled again totaling 304 million Internet users worldwide.[5] As of March 2002, there were 446 million Internet users worldwide.[6] It is estimated that by 2005 there will be one billion Internet users worldwide with 700 million located outside North America.[7]

The increase in worldwide Internet use has also created a potential threat to the national security of the United States. The global "hot spots" which are Asia, the former Soviet Union, and the Middle East have also shown a substantial increase of Internet users.

At the end of 2000, the Asia-Pacific region had 78 million subscribers; that is an increase of 65 percent over the 1999 figure of 47.4 million subscribers. As of March 2002, the Asia-Pacific region had 120 million Internet users. By 2005, Japan and China combined will have approximately 151 million subscribers, representing about 61 percent of the total Asia-Pacific subscriber base. India from 2001 to 2005 will see an average subscriber growth of 44 percent a year according to Dataquest, a research group that tracks Internet statistics. If the numbers hold true India will have the fourth largest Internet market, behind China, Japan, and South Korea.[8]

China, the biggest threat to U.S. national security in the region, had 54.35 million Internet users at the end of September 2002 according to the Chinese Ministry of Information Industry. The new figures indicate that there are 20.56

million computers connected to the Internet and nearly 82,000 local websites in China. [9]

The former Soviet Union has also seen the increase in Internet users. In 2001 the number of Internet users had doubled to a total of 18 million users. According to a report from the Russian IT Public Center the number of 'regular' Internet users grew to 8 million. [10]

New research from the Information Society of Ukraine says that 2 million Ukrainians will be online by the end of 2002. Currently there are 280 Internet Service Providers in Ukraine, with 80 of them based in the country's capital. [11]

The number of Internet users in the Middle East has increased dramatically within the past 3 years. In 2000 the number of Internet users in the Middle East was approximately 2 million. By March 2001 the number of Internet users totaled 3.54 million. As of March 2002, there were 6.3 million users throughout the Middle East.[12]

The United Arab Emerites between 2000 and 2001 saw a growth of Internet users at 57%. The number of subscribers in the country grew from 140,000 to 220,000 by mid March 2001.[13] Currently there are 920,000 Internet users in the UAE. That is 38.3 percent of its current population using the Internet. That is almost equal (per capita) to the United States which has 38.92 percent of its population using the Internet.[1]

Concept of Cyber Terrorism vs. Traditional Terrorism

The definition of cyber terrorism is the ability through the use of a computer to create mass destruction to a political or economic institution that sustains the daily functions of a society, or to create fear among its members.

One difference between traditional terrorism and cyber terrorism is that traditional terrorism becomes known when an attack occurs. However, with cyber terrorism one may not know the attack has taken place. It takes a cyber terrorist seconds to break into a computer, transfer the information, and leave without a trace and that attack may not become known for hours, days or even years. More importantly, cyber terrorism provides a window of opportunity for terrorist groups, drug traffickers, organized crime, and anti-US nation states that were once only able to cause minimal damage, to wage war against the United States and be successful in a new way.

Recently, there is a direct relationship between political conflicts and increased cyber attack activity. United States and allied military strikes may result in cyber attacks against American and allied information infrastructures with significant economic, political, or symbolic value.

A week after the September 11, 2001 terrorist attack a cyber attack was striking leading financial services firms a few blocks away from the World Trade Center site. The attack was called "NIMDA." It was an automated attack, a blend of a computer worm and a computer virus; it propagated across the nation with enormous speed and tried several different ways to infect computer systems it invaded, until it got in and destroyed files. It went from nonexistent to nationwide

in an hour, lasted for days and attacked 86,000 computers. NIMDA caused significant problems in well protected industries, forcing firms off line, shutting down customer access, and requiring some firms to rebuild systems entirely.[15]

Subsequent to the April 1, 2001, mid air collision between an American surveillance plane and a Chinese fighter aircraft, Chinese hacker groups immediately organized a massive and sustained week-long campaign of cyber attacks against American targets. Approximately 1200 U.S. web sites, including those belonging to the White House and other government agencies, were subjected to Denial of Service Attacks or laced with pro-Chinese images.[16]

Cyber terrorism can be more destructive than traditional terrorism. A cyber terrorist could alter the formulas of medication at a pharmaceutical manufacturer or change the pressure in the natural gas lines, causing a valve failure; cyber terrorism is not just an inconvenient destabilizing of a nation's infrastructure.

Cyber terrorism is a not a new concept. In fact, it started with the first invention of a computer. Not much is known to what extent terrorist organizations will use cyber terrorism. In recent years terrorist organizations have used the Internet as a means of communication within the organization. Terrorist organizations such as the Al-Qaida Network are using popular web sites to post encrypted messages that detail plots for guerrilla activities. [17]

Security experts said some messages are scrambled using free encryption programs set up by groups that advocate privacy on the Internet. These messages are then decrypted using a code known only by the recipient and sender.[18]

The terrorist organizations found that computers provide increased anonymity, mass recruitment potential, and a cost effective way of carrying out an act. None of these activities is easily detected or readily countered, and thus such activities enable terrorist organizations that use computer technology to create viable support structures to further their tactical and strategic goals.

Computers enable terrorist organizations to organize without the knowledge of federal authorities. This will lead to stronger and more resilient organizations that will become deadlier than earlier terrorist organizations.

In previous decades, terrorist groups were initially constrained because the accumulation of sizeable resources was inevitably linked to sufficient manpower and the ability to keep growth activities clandestine. Cyber terrorism has enabled terrorist organizations to become less reliant on external sponsors such as nation states.

Summary of Chapters

The second chapter will focus on an individual called a "hacker." A hacker is the main focus in anything relating to cyber terrorism since a hacker is the person who performs the cyber terrorist attack. In the chapter, I will focus on the psychological makeup of a hacker. Also it shall attempt to answer the question, why does an individual want to break into a computer? For the answer to this question, I look at the writings of Nicholas Chantler who did a case study profiling a hacker. His writings analyze the hacker from the standpoint of social environment, home life, and intelligence level.

I will also look at how a hacker has similar characteristics to a physical terrorist. The writings of Rex Hudson looks into why a person becomes a terrorist. The similarities between a terrorist and a cyber terrorist are in most cases parallel to one another.

The second chapter will also focus on an information warfare operation. This is when the actual cyber attack occurs. There are two different views of the operation. One is from the defensive player who is the network or systems administrator of the institution. The other one is from the offensive player who is the cyber terrorist that wants to create an advantage over the defensive player.

The third chapter describes two current policies set forth by the United States Government to combat cyber terrorism. The first is the "National Strategy to Secure Cyberspace" proposed by the committee created by Executive Order 13231 by President George Bush. This strategy outlines what is needed to secure cyber space. It calls for joint cooperation between the public and private sectors and for every citizen to do his or her part to secure cyberspace.

The second policy is the Patriot Act which was signed into law by President Bush on October 26, 2001. The act calls for increased monitoring of computer systems and greater authority for investigations by law enforcement officials. The act has come under fire by privacy organizations believing that the provisions in the act will violate an individual's right to privacy.

In the second part of the chapter I look at the pro's and con's of each policy. In this section, I discuss the problems with the policies and address the concerns of the privacy organizations. I also look at possible violations of the

First and Fourth Amendments if the provisions of the Patriot Act are implemented.

In chapter four, I discuss my proposal for a National Information Policy. I look at why a National Information Policy should be created, the components of such a policy, and the benefits it can have for society. Each component of the policy will provide protection against a cyber attack which would cripple the nation's infrastructure, while at the same time protecting an individual's right to privacy.

CHAPTER 2

PRINCIPLES OF COMPUTER SECURITY

History of Hacking

Today, the individual engaged in a cyber terrorist attack is called a hacker. However, the term 'computer hacking' originated in 1958 when a student at the Massachusetts Institute of Technology named Peter Samson hacked into the keypunch machine that punches holes into punchcards for the IBM 704 Computer (mainframe computer).[1] The definition of a computer hacker was a person who gets a deep sense of enjoyment and satisfaction from immersing themselves into understanding the way computer software and hardware works, through practical examination and experimentation. But the term has evolved, so that in today's society a hacker is seen as a pirate, one who infiltrates an computer network unauthorized in order to create destruction or some other harmful outcome by illegal means.

The first computer crime was in 1973. It was a fraud case in America where a computer was used illegally to generate a large number of bogus accounts. It was considered that the crime could not have been committed without the use of a computer.[2]

The culture of a hacker has changed from generation to generation corresponding with the technology generations. The first generation of hackers

was based on the East Coast of the United States, developing software. In 1969 two employees at the Bell Labs' think tank came up with an open set of rules to run machines. Their source code was a response to the desire to complete computing tasks more quickly on the mainframe systems. They called their standard operating system "UNIX."[3]

The second generation, the 1970s hackers had expanded across the United States. By this time the computers were going into the great wide open society, and computer hacking was quickly becoming mainstream computer culture. In 1971 a Vietnam Veteran named John Draper discovered that the whistle in the Captain Crunch cereal boxes perfectly reproduced a 2600-megahertz tone. All a person would have to do is blow the whistle into a telephone receiver to make free long distance calls. In 1978 Randy Seuss and Ward Christiansen created the first personal-computer bulletin board system. It provided hackers an open forum to discuss and swap ideas.[4]

The next generation of hackers was based in North America and Europe. These were young adolescents who were the first recipients of the personal computer and were copying and selling the first computer games. Hollywood explored the world of computer hacking through the 1983 movie "War Games." For the first time the general public became aware of hackers and what they could accomplish through the use of computers.[5] The 1980s also saw more people exploring the online world. ARPNET was evolving into the Internet and this decade also saw the rise of bulletin board systems.

The fourth generation had inherited a world centered on the personal computer and online communication. This new generation shared the same 'obsessions' as their predecessors. But the difference is they viewed 'hacking' not as an honorable trade but as a form of breaking and entering with the intent to cause destruction.

As I have shown the original intention of a computer hacker was to increase production time while making the work easier to input for the end user. However, throughout the years as more people used computers and they became a fixture in modern society, a "hacker" (shown in the examples below) became a person whose intention is to create chaos and destruction. In fact, if the original definition of a hacker remained the same throughout the years the concept of cyber terrorism would never exist.

In the summer of 1994 a gang masterminded by a Russian hacker broke into Citibank's computers and made unauthorized transfers totaling more than $10 million from customers' accounts. Citibank recovered all but $400,000 dollars. In the second week of February 2000 some of the most popular Internet sites (CNN, Yahoo, E-Bay, and Datek) were subjected to "Denial of Service" attacks. Their networks clogged with false requests sent by multiple computers under the control of a single hacker. These commercial sites crashed and lost millions in sales. In May 2000, a new virus appeared that spread rapidly around the globe. The "ILOVEYOU" virus infected image and sound files and spread quickly by e-mailing copies of itself to all individuals in an address book.[6]

Psychological Makeup of a Cyber Terrorist

In 1996, Nicolas Chantler was one of a few people to look at a computer hacker from a psychological approach. His book A Profile of a Computer Hacker looks at a hacker from the perspectives of family environment, intelligence level, and social peer interactions.[7] He states that hackers come from unhappy family backgrounds and have in the majority of cases, high levels of non-achievers and in many cases dropouts. They find school unchallenging and believe it is a waste of time where their time could be put to use somewhere else. Needless to say hackers are bright and known to have an above-average IQ. They are able to focus intensively for an extended period of time. They are focused on understanding, preparation, and control. It is difficult for hackers to develop relationships with people since their adversary, partner, friend, advisor, and witness is the computer. They are often shy, overweight, and picked on at school and use the computer as means of an escape. Hackers rely on their skills to boost their self-esteem, to enjoy being renowned among fellow hackers.[8]

Hackers create a 'handle' or 'stage name' to hide their lack of self-esteem. Some of the more famous hackers include Captain Crunch, Optik Surfer, The Mad Crasher, Phiber Optik, Byte Ripper, Rential Burn, SLH (Satan Little Helper) and the Blue Boxer. They refer to each other by this assumed identify, frequently not knowing the real identity or 'eye balling' other hackers unless they are in close residential proximity. It is believed that the fiercer the handle, the meeker the kid behind it. Hackers believe that there is a huge element of role-playing in hacking.[9]

Hackers feel secure operating under this masquerade, using the keyboard and modem as their means of communication. They view themselves as electronic freedom fighters. They build an imaginary world based upon science fiction that features the underworld of high technology. Cyber punks who become streetwise in technology and communication imagine they exist in a conceivable near-future realm, where they take on the identity of science fiction characters. Hackers create their own virtual reality – an imaginary cyberpunk world where they can live out their science fiction fantasies.[10]

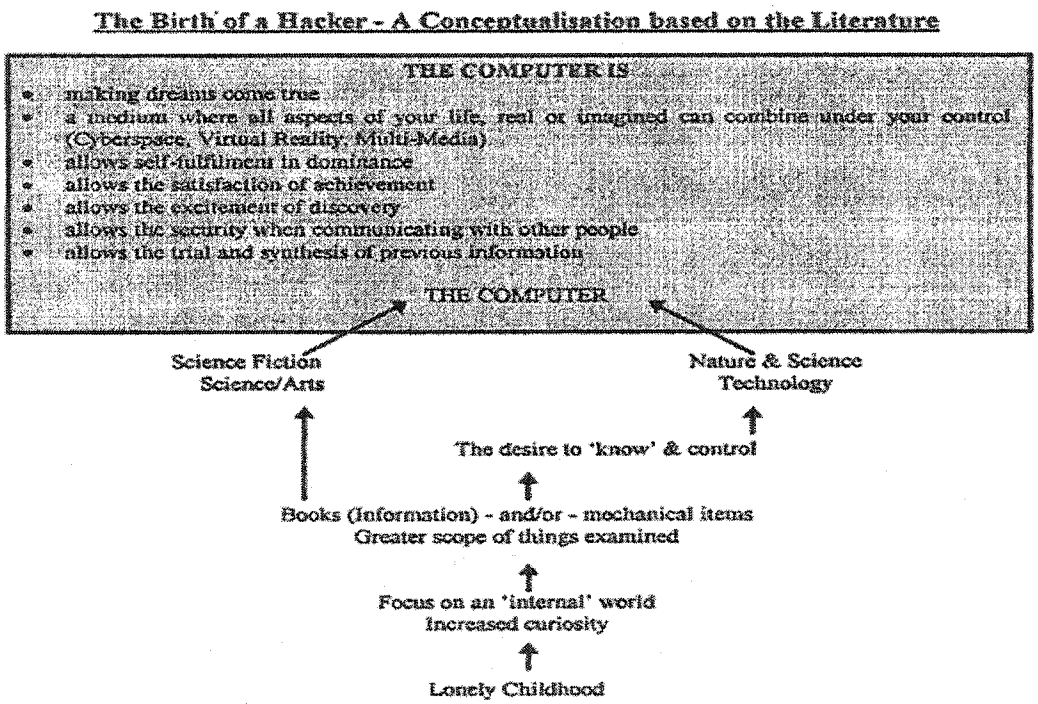

Figure 1: The Psychological Aspects of a Hacker. Source: Nicholas Chantler, "Profile of a Computer Hacker" (Ph.D. diss., University of Queensland, 1996).

The most common motivations for hackers are straightforward curiosity, fascination, and intellectual challenge. The illicit thrill of outwitting a system's

security is compounded by the excitement of the potential for future expeditions. Hackers are seduced by the thrill of exploring computer networks. Thriving on the sense of power and knowing they are on the edge of the law and getting away with it drive them.

Marc Rogers, a behavioral sciences researcher at the University of Manitoba in Winnipeg, Canada and a former cyber detective, identified four categories of hackers: 1. Old School Hackers – these are your 1960s style computer programmers from Stanford or MIT for whom the term hacking is a badge of honor. They are interested in lines of code and analyzing systems, but what they do is not related to criminal activity. They do not have a malicious intent, though they may have a lack of concern for privacy and proprietary information because they believe the Internet was designed to be an open system. 2. Script Kiddies or Cyber-Punks – what the media most commonly calls "hackers." As an age group, they can be between 12 and 30 years old, they are predominately white and male and on average have a 12^{th} grade education. They are bored in school and very adept with computers and technology. They download scripts or hack into systems with the intent to vandalize or disrupt systems. 3. Professional Criminals or Crackers – these guys make a living breaking into systems and selling the information. They might get hired for corporate or government espionage. They may also have ties to organized criminal groups. 4. Codes and Virus Writers – they like to see themselves as an elite. They have a lot of programming background and write code but will not use it themselves. They have their own networks to experiment with, which they call

"zoos." They leave it to others to introduce their code into "the wild," or the Internet.[11]

Psychological Makeup of a Terrorist

Psychologist Eric D. Shaw created "The Personal Pathway Model" to analyze why a person becomes a terrorist. The Personal Pathway Model suggests that terrorists come from a selected, at risk population, who have suffered from early damage to their self-esteem.[12]

As a group Shaw believes they have been unsuccessful in obtaining a desired traditional place in society, which has contributed to their frustration. A membership to a terrorist group gives this type of individual a sense of potency, an intense and close interpersonal environment, social status, potential access to wealth and a share in what maybe a grandiose but noble social design.[13]

Jerrold Post's conclusion is similar to Eric Shaw's conclusion. Post also believes that for the new recruit, the terrorist group becomes a substitute family, and the group's leaders become substitute parents. The key motivation for membership in a terrorist group is the sense of belonging.[14]

A typical member of a terrorist group is between the ages of 20-25 years. However in countries that are involved in ethnic, political, or religious conflict the members are a lot younger. A terrorist has a more than average education. In fact, 66% of the terrorists in the study had university training and came from middle-class to upper-class backgrounds. A good example is the current leader

of the Palestine Liberation Organization (PLO), Yassir Arafat. He was a graduate engineer.[15]

Psychological Summary

As shown there is not much difference from a psychological standpoint between a terrorist and a cyber terrorist. Both groups of individuals come from an environment that contributed to their low self-esteem and the need to be wanted and accepted by others. By bringing these types of individuals together in a group gives each one of them a sense of identity and the ability to strike back at a society in which they believe has done them an injustice. This type of mindset is dangerous and needs to be prevented at all costs.

Information Warfare and Principles

When an individual or group engages in a cyber attack, the attack itself becomes known as information warfare. Information Warfare is made up of two players: an offensive player (cyber terrorist) and a defensive player (computer security officer). An offensive player launches an operation against a particular information resource, the defensive player aims to defend against the operation.[16]

An offensive information warfare operation is one that targets or exploits a particular information resource with the objective of increasing its value to the offensive player and decreasing its value to the defensive player. The gain could be financial, such as targeting a bank; political, targeting government systems; or

a single-issue objective, targeting an abortion clinic. If the offensive player does not believe there is a potential gain in value then offensive information warfare is not likely to be practiced.[17]

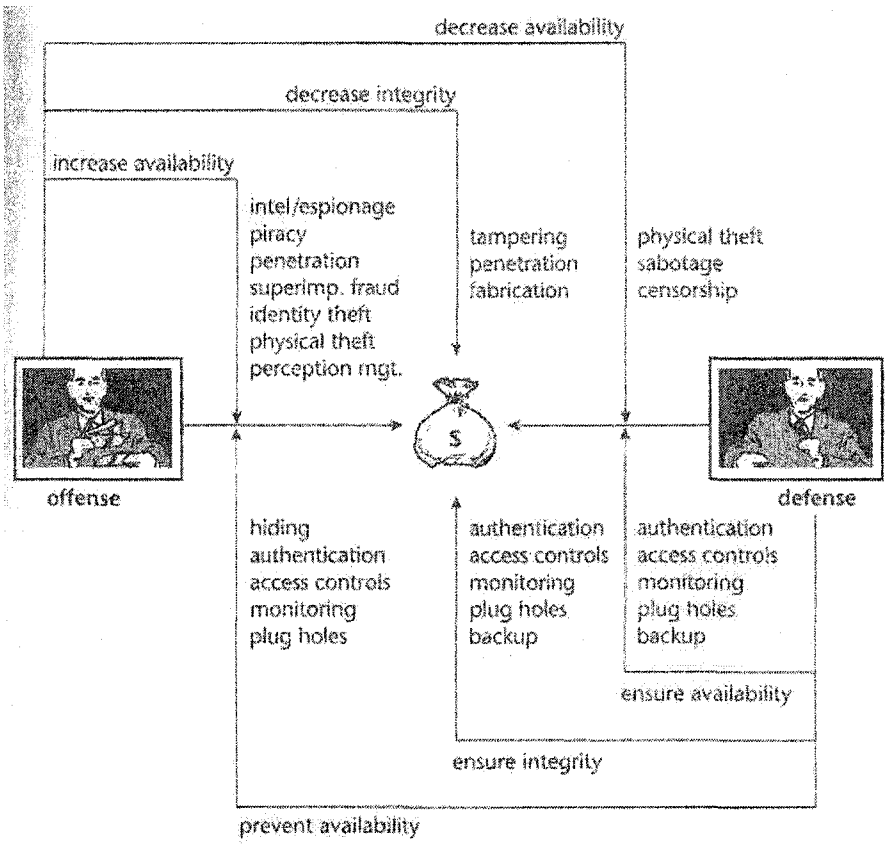

Figure 2: A diagram showing an Information Warfare Operation. The money bag represents the value to both the offensive and defensive player. Source: Dorthory Denning, Information Warfare and Security (New York: ACM Press, 1999).

Defensive Information Warfare

Defense is the most important aspect in information warfare. A strong defense is needed to prevent and deter an attack or, if an attack occurs, to minimize the damage. 1. detection along with prevention, 2. deterrence and 3. deception are the three most important means of protection.

1. Detection can be performed by either a person, device, or program. Prevention includes four components of security: (a) document security deals with who handles computer documents, disks, and hardware; (b) personal security includes knowing who has access to the system as well as the correct security level; (c) hardware security includes maintenance procedures of the network and hardware identification devices; and (d) software security includes procedures that need to be established to control the design and changes to software. It includes the procedures to guard against, detect, and kill any viruses, and also the procedures to issue and control passwords.[18]

A firewall is an example of detection and prevention. It control access and blocks the flow of certain packets while monitoring for intrusions and denial of service attacks. Certain patterns of activity must be understood as objects of detection. These include unexplained system crashes, restarts, and behavior or any performance which can be a sign of SYN Flood or some other denial of service attack. Even multiple sign on attempts to a computer terminal could suggest that someone is trying illegally to enter an account.

After software installation, monitoring of software behavior, which includes interactions with other software programs and operating systems, must continue on an ongoing basis. Security problems can arise any time information resources are updated and reconfigured or when new resources are added or old ones removed.

2. Deterrence is the essential first order of a defensive objective. A deterrence strategy is a warning to those who would attack to expect an attack in return.

A strategy of deterrence has three prerequisities: (1) the incident must be well defined; (2) the identity of the perpetrator must be clear; and (3) the will and ability to carry out punishment must be believed.[19]

There are two types of deterrence that the United States can use to prevent an attack: general and focused. General deterrence stems from maintaining the capability and will to inflict severe damage in retaliation against those who would disturb the peace. Merely by supporting a large and highly capable military, the United States conveys its ability to punish those who would transgress against it. General deterrence does not require the communication of a specific threat against aggressors; its effectiveness relies rather on the presence of an arsenal of tangible capabilities.[20]

Aside from punishment, general deterrence can work through denial. It should be made clear to any cyber terrorist or any anti-US organization that they will not be permitted to attain their objectives; recognizing that they cannot succeed, they are deterred from making the attempt.

Focused deterrence operates at a different level of specificity. It recognizes that sometimes general deterrence does not work, that posturing without reference to a particular objective will be viewed as weak or irrelevant, so that a focused or specific deterrent threat or statement is required. For example,

the United States should have issued a focused deterrent statement against Iraq warning them of the consequences of invading Kuwait.

3. The term 'deception' includes techniques such as concealment, manipulation, distortion, falsification of indicators, and decoys. The objective of deception in cyber defense terminology is to create as much confusion and uncertainty as possible for potential attacks, regarding the value and location of critical information systems and resources.

Outline of an Information Warfare Campaign

Since the Persian Gulf War the military has become aware of information warfare and how it can be incorporated into a military campaign. The functions that will be used in an information warfare campaign are very similar to what the military currently employs. The difference is in the execution of the campaign.

Survey Function

Survey is the first function. Survey involves information collection. This can be done through human intelligence, technical intelligence, counter-intelligence, and open source intelligence.[21]

Open source intelligence is the most used type of information gathering in information warfare. This includes accessing message boards, websites, and downloading encrypted messages. As discussed in the previous section "hacking" is another way of surveying information.[22]

Information Fusion Function

The second function of information warfare is assessing the information. To assess information one must gather the information collected in the previous step and compile the information. Another name used for this process is "information fusion," the combining of information into a battle space picture, which the information warrior can use.[23]

Once the data is received, it is evaluated by intelligence analysts to determine its meaning. Specialized software programs, databases, imagery views, and encryption programs are used to decode the data.

Upon assessing the information the next step is to analyze the system. This includes analyzing one's own system as well as the enemy's system. This is critical for a successful operation because one must look at the information architecture, which includes the nature of data in the system and the protocols and methods for data transmission. It also allows the hacker to understand how much time he or she has inside the system before being detected.[24]

This step is very important because in order to attack or defend from an attack one must know the abilities and limitations of his own system as well as the abilities and limitations of his opponent's system. For example, if you were going to fight another person, before the first punch is thrown you would ask yourself, "Can I win?" To answer this question you first would analyze your own abilities and limitations then you would analyze your opponents abilities and limitations. Finally, you would conclude whether or not you can win the fight.

Command Function

The command function is the third function of an information warfare operation. In this function one would conduct planning and determine the best courses of action. Information warriors would employ manual or automated planning systems and target databases to produce an overall information warfare campaign.[25]

Also in this function one would identify the system's center of gravity. At this step, the hacker would narrow his or her focus. The goal is to identify the critical nodes and linkages in an enemy's information system, which, if struck, would accomplish the objectives he or she has laid out.[26]

At the same time however, the information warrior must identify the critical nodes and linkages in his or her own system, which, if protected, would prevent an enemy from accomplishing his or her objectives.[27]

Control Function

The fourth function is the control function. It analyzes received tasking orders, readies assists, responds to the threat and situational changes, and reports the results back to the command function.[28]

Under the control function the tools that will be used are selected for the attack. The selection of tools that will be used is based upon several factors. First is availability. The information warrior must determine which tools are available for his or her use. If a tool is not available but is deemed critical, it must either be requested or a different selection must be made.[29]

The second factor in tool selection is the effect the planner wants to achieve through targeting. It is important to consider the full range of options and avoid the trap of only targeting for 100% destruction. This can result in wasting resources and unnecessary risk when mere neutralization might have sufficed. It maybe desirable to affect the elements of the system one is attacking for a long period of time.[30]

The third and final factor in tool selection is assessing the target to determine its vulnerability to attack and attendant risks in attacking it. The planner must select tools which can feasibly thwart defenses and affect the target without undue risk. It must be evaluated in a cost-benefit analysis at all levels.[31]

Different tools, used in different ways, can produce a variety of effects from destruction to neutralization, from long term to short term. The information warrior must select and employ tools based on the right combination of effects, which will allow him or her to obtain the objectives at minimum cost and risk.[32]

Execution Function

The fifth function of information warfare is the execution of an attack. Execution is divided into two categories: information attack and information defense. The purpose of an information attack is to create a combination of "data overload" and "data starvation" in the offensive player's system while protecting your system at the same time. A data overload occurs when a system cannot handle the information coming into it or flowing through it. One type of data overload is a denial of service attack. Data starvation is when adequate inputs to the computer cease.[33]

When a multitude of information points are attacked in parallel, two results occur in the information system. First, the disrupted points no longer provide information to the downstream functions and thus "starve" the parts of the system to which they are connected. Secondly, segments of the information system which are not disrupted have to carry the existing load of the entire system, as well as the increased traffic flow from real or artificially induced disrupted reports.[34]

Assessment Function

The sixth and final function of information warfare is to assess the effects of the attack. The purpose of this function is to provide feedback on the overall operation. In order for feedback to occur one must compare actual effects with those desired, and must compare the overall impact on the system with the desired end state. This provides two feedback loops, which will allow the planner to adjust efforts as necessary.[35]

The first loop is the comparison of effects achieved in targeting or protecting individual elements with the desired effects. If surveillance reveals the effects were as desired, the planner should move on to other objectives. However, if the desired effects were not achieved, the planner must determine if the effect actually achieved (if any) is sufficient or if restack is necessary. The planner must also evaluate why the effect differed from expectations to determine if the tool applied was inappropriate or the risk and vulnerability assessment was defective.

The second assessment feedback loop involves the continuous comparison of the effects on the system as a whole with the desired end state. This provides the planner with a yardstick approach for measuring progress toward the campaign's objectives. It can tell one when to end the campaign and perhaps devote resources elsewhere.[36]

Chapter 2 Summary

The second chapter has shown the motivations as to why an individual would want to hack into a computer system. Nicolas Chantler's psychological approach to the mind of a hacker has shown that the intelligence of a hacker and the lack of a stable environment combine to produce a potentially dangerous person. The amount of destruction and impact this person can have on computer systems has endless possibilities. That is why there must be safeguards in place to ensure that this type of person does not gain success at any level.

The second chapter also shows how a traditional terrorist and a hacker mindset are similar. Both believe they are outcasts of society. When they form a group, it is a group of individuals who want to strike back at a society which they believe has done them an injustice.

The third part of the chapter shows with the right planning and tools how easy it is to create an information warfare operation. This type of operation has been standard for a traditional military operation for thousands of years. But in order to convert the operation model to include an information warfare attack, the amount of time to complete the operation model is less than it would be for a

traditional military operation model. This causes individuals to change their mindsets about traditional warfare to where a response is required within seconds of action and countermeasures must be at one's immediate disposal.

The next chapter shows what the current policy of the United States Government is to combat the threat of cyber terrorism.

CHAPTER 3

CURRENT POLICIES ON COMPUTER SECURITY

Section I: Cyber Security Plan

The National Strategy to Secure Cyberspace is a draft plan proposed by the Bush Administration in response to an increased threat of a cyber attack to the United States infrastructure. As stated in the statement of national policy the integrity of the national economic and social fabric over the long term requires attention, not only to the security of information systems, but also to the related societal structures on which those systems depend.[1]

The authors of the plan believe that the security of cyberspace is the responsibility of everyone from the home user to the federal government. Each individual and organization has a responsibility to secure its own portion of cyberspace. [2]

For individual and corporate responsibility the authors have developed six tools for empowering people and organizations. These are 1. Awareness and Information, 2. Technology and Tools, 3. Training and Education, 4. Roles and Partnerships, 5. Federal Leadership, and 6. Cooperation and Crisis Management. [3]

The Home User and Small Business

The strategic goal is to empower the home user and the small business person to protect their cyberspace and prevent it from being used to attack others. The authors believe the goal can be achieved through the following: 1. raising cyber security awareness of the home user and small business, including children and students; 2. making it easier for home users to keep current with anti-virus software, software patches, and firewalls, perhaps through activity by the Internet Service Providers; 3. encouraging and helping facilitate the installation and use of firewalls on all broadband Internet connections, such as cable modems, DSL, satellite and wireless; and 4. bringing cyber security resources closer to the users through local organizations and educational courses. [4]

The first step to security awareness of the home user and small business is tough password protection. Using a tough password means creating a password that is not easily accessible by other people, especially hackers. Hackers commonly break into computer systems where users have created passwords that are common terms. This includes pet's name, social security number, birth date, family member's name, favorite color, or favorite food. [5]

The authors believe that strong passwords should have at least eight characters, a mix of upper and lower case letters, a random mix of letters and numbers, and keyboard symbols.

The second step to security awareness is anti-virus software, software patches, filtering, and firewalls. New viruses appear weekly and the new ones

are the most frequent source of damage. Users should maintain an updated virus protection program. The authors believe that the user should buy an anti-virus software program and enroll with the antivirus company for weekly update to the program. [6]

Many commonly used software programs are regularly discovered to have security holes or flaws. In this instance "software patches" are needed to fix the problem. Software companies issue alert notices. These alert notices require the user to go to the company's web site to discover the problem and the solution. Once the solution is found the user nominally downloads a software patch and installs it on his/her computer. [7]

The authors encourage parents to filter software to manage their children's Internet usage. The filter software acts like a guardian that says 'yes' or 'no' as to which Internet sites children can visit. [8]

The authors also believe that home computer users should purchase a firewall, especially home users who have a cable modem, DSL Satellite connections, or other high speed connections. Firewalls can be easily configured to close many doors to the Internet that all computers have, leaving open only the few that people use. A user can specify what Internet programs are trusted to enter and require all others to knock and be granted permission. [9]

Large Enterprises

The strategy goals of the National Strategy regarding enterprises are to encourage and empower large enterprises to establish secure systems. This goal can be achieved through a range of voluntary initiatives including: 1. raising the

level of responsibility; 2. creating corporate security councils for cyber security, where appropriate; 3. implementing A.C.T.I.O.N.S. (see below) and best practices; and, 3. addressing the challenges of the borderless network, mainframe security, instant messaging and other technologies. [10]

In order to raise the level of responsibility, the company's board of directors plays a vital role in the corporate system. Shareholders ultimately own corporations. Corporate boards are accountable to shareholders, and, in turn, managers are accountable to the board. Raising the responsibility for cyber security to the level of the board of directors can have significant enterprise results. The board can better understand its enterprise by asking a series of questions about the sufficiency of the organization's security structure and controls. To better understand the scale, scope, and effectiveness of enterprise security, some boards, through an appropriate board committee, require periodic reporting by management. [11]

Today's diffuse security threats require new thinking and approaches. For example, some large enterprises may want to consider creating corporate security councils consisting of key members of the company with security-related responsibilities. Corporate officials with risk management and security-related responsibilities could form the core of such a team. [12]

Finally the authors of this plan believe that "A.C.T.I.O.N.S." can be undertaken to facilitate the integrity, reliability, availability, and confidentiality of the enterprise. They consist of Authentication, Configuration management,

Training, Incident Response, Organization network, Network management, and Smart management. [13]

The Federal Government

The security of the federal government is the collective responsibility of its departments and agencies. Accepting anything less than excellence in Federal computer security places the nation and the American people at excessive risk.[14]

The Office of Exercise Budget and Security Oversight issued a report to Congress that identifies six common government wide security performance gaps: 1. Lack of senior management attention; 2. Lack of Performance Measurement; 3. Poor security education and awareness; 4. Failure to fully fund and integrate security into capital planning and investment control; 5. Ensuring that contractor services are adequately secure; and 6. Failure to detect, report, and share information on vulnerabilities. Other key gaps include: Authentication: Keys to Cyber Security such as passwords and Inconsistent Contingency Planning. [15]

The federal government must have a comprehensive and cross-cutting approach to improving cyber security. The authors believe that cyber security is not a "one-size-fits-all" solution. However, there are three elements that are central to attaining and maintaining robust cyber security for the federal government. These include: 1. identifying and documenting enterprise architectures; 2. continuously assessing threats and vulnerabilities, and understanding the risks they pose to agency operations and assets; and, 3.

implementing security controls and remediation efforts to reduce and manage those risks. [16]

As a matter of OMB policy, each agency must identify and document their enterprise architecture, including developing an authoritative inventory of all operations and assets, and all agency Information Technology (IT) systems, critical business processes, and their inter-relationships with other organizations.[17]

Agencies must continuously assess threats and vulnerabilities and understand the risks they pose to agency operations and assets. Commercial automated auditing and reporting mechanisms are now available to validate the effectiveness of the security controls across a system and are essential to continuously understand risks to those systems. [18]

Automated tools on agency networks could continuously assess system vulnerabilities, collect and analyze firewall and intrusion detection audit logs, audit configuration and security policy controls, and automatically report the results to the Federal Computer Information Resource Center (FedCIRC). The authors believe automated tools can be helpful in analyzing data, providing forward-looking assessments, and alerting agencies of unacceptable risks to other operations. [19]

The implementation of security controls that maintain risk at an acceptable level and test the controls to ensure that they continue to be effective can often be accomplished in a relatively brief amount of time. However, the remediation of vulnerabilities is a much more complex challenge. [20]

The framework for the federal government consists of an 11 step approach to secure cyberspace. These steps are : 1. hold agencies accountable; 2. Establish an Office of Information Security Support Services; 3. develop a federal cyber incident response plan; 4. test agency security preparedness; 5. explore creation of a separate federal telecommunications and information systems infrastructure; 6. consider developing specific criteria for independent security reviews and reviewers and certification; 7. overarching reviews by the Board's Executive Branch Information Systems Security Committee; 8. Gap Analysis of Current Policies and Processes; 9. risk grading by agencies; 10. set uniform security practices or benchmarks for similar operations, assets, and systems; and 11. have cross government steps. [21]

The authors have laid out how information technology can be integrated in the newly created Office of Homeland Security. They divided the goals into two parts: major strategic goals and immediate objectives.

The strategic goals are: 1. create collaborative partnerships with State and local governments and the private sector; 2. ensure adoption of leading-edge information technologies as offensive weapons in the prevention and detection of terrorism; 3. drive national and international information integration and information delivery standards; and 4. develop innovative service delivery models and business models that enable government to use information held outside the government arena.[22]

The immediate objectives are: 1. lead the integration of information essential to homeland security across federal agencies; 2. drive the integration of

information essential to homeland security among and between Federal, State, and local government, and the private sector; and 3. guide the enablement of the "National Strategy for Homeland Security" through appropriate use of information technology capabilities, products, and services. [23]

State and Local Governments

State and local governments play an important role in the emergency law enforcement sector. Emergency Law Enforcement Services (ELES), as a critical infrastructure sector, is included within the emergency services sector. The continued operation of the ELES sector during a time of crisis is essential to the rule of law, the protection of the general welfare, the preservation of civil liberties and privacy rights, and consequence management. [24]

More than 18,000 Federal, State, and local agencies comprise the ELES sector. Those agencies developed the ELES sector critical infrastructure protection plan which presents the sector's initial strategy for ensuring its continuing ability to perform critical law enforcement functions. [25]

Private Sector

The private sector plays a central role in securing cyberspace because it owns and operates a vast majority of the nation's infrastructures and the cyber systems on which they depend. The authors believe cyberspace security is a shared responsibility. No single industry is responsible for its security and no government entity can protect it. [26]

During the past decade American infrastructures have integrated information technology and cyberspace into almost every aspect of their

operations. The rapid integration of IT has yielded profound efficiencies, promoted innovation, and increased service reliability. Once distinct infrastructures, which were isolated by closed proprietary systems, are now tightly integrated with one another. This integration has created many new and complex interdependencies. The authors believe that in order to assist the private sector to secure cyberspace there must be a successful public-private partnership. [27]

Global Priorities

The strategic goal is to work with the international community to ensure the integrity of the global information networks that support critical U.S. economic and national security infrastructure. This goal can be achieved through a range of initiatives. The United States will: 1. promote the development of an international network to identify and defend against cyber incidents as they begin; 2. encourage all nations to pass adequate cyber security laws so that U.S. law enforcement can investigate and prosecute cyber crime committed against the United States and its interests, whether it originates domestically or abroad; 3. work through international organizations to foster a "Culture of Security" worldwide, to ensure the long-term security of the global information infrastructure; and 4. promote the international adoption of common international technical standards that can help assure the security of global information infrastructures. [28]

The United States will promote a wide range of initiatives to enhance cyberspace security globally and will disseminate key policy messages through

the full array of bilateral, multilateral, and international fora, as appropriate. These initiatives will: build real-time, "24/7" watch-and-warning networks to identify incidents and stop them establish and link a network of cyberspace security coordinators in each nation, use international organizations to promote regionally the principles and standards essential to fostering a global culture of cyberspace security, assist nations in developing the laws and acquiring the skills to effectively investigate and prosecute cyber crime across international borders, and foster collaboration among the best minds in the world on long-term solutions to cyber security. [29]

Section II: An Analysis of the Cyber Security Plan

The national strategy is in my opinion a strategy to neither secure cyberspace nor combat cyber terrorism. It is more like a plan with a set of ideas with no clear objective on how to solve the problem. The plan was written without input from the private sector and never took into account the education of the home user. It would be impossible for everyone "to do his or her own part to secure cyberspace" if no one understands what his or her role is.

Home User

The first part of the plan looks at what home users can do to protect themselves from an attack. However most of the policy requires the home user to be very computer literate, which most of the people who have a home computer are not. Most people who have a computer at home use it for e-mail and basic internet and word processing functions. The plan calls for home users to install a

firewall and an anti-virus software, both of which require an initial purchase and yearly operating costs. The first problem with this idea is that people who use the computer for basic functions will not understand why these two software programs are necessary. The second problem is the cost associated with the two programs. On the average a firewall and anti-virus software costs between $50-80 to purchase, and yearly renewal costs between $20-45. How do you justify these purchases to a user who uses the computer for basic functions? The third problem is that most home users still use a dial-up connection so a firewall would not be of any use to them.

The plan also calls for home users to implement tough passwords and not to use passwords that people can easily guess. The first problem is that if a person creates a password that he or she can not associate with they will likely forget the password.

The second problem is that there are other easier ways someone can break into a computer. Spyware programs such as gator.com or hotbar.com install themselves on an individual's computer without their knowledge or are a required installation in order for a program like Kaaza (peer-to-peer file sharing network) to operate. In the case of Kaaza, if the spyware part of the program is deleted the program will malfunction and in some cases delete shared ".dll " files which are used in programs like Microsoft Office and other Windows programs.

Spyware programs are created by marketing and bulk email agencies to collect information and sell it for a substantial price to third party vendors. The vendors will then target the user to buy their products or services.

The problem with spyware programs is that they collect personal and private information without the users' knowledge. The information collected can be a combination of e-mail addresses, Internet Addresses (ISPs), and programs on the computer that the individual uses such as documents, graphics, and/or other files.

If this information gets into the hands of a hacker, he or she has the tools and information to break into a computer without the user's tough or strong password.

Private Sector and Large Enterprises

The major reason as to why the national security plan would not accepted by the private sector has to do with economics. Since the dot com bust of 2000 companies do not look at information technology as a profitable commodity. According to the 2003 IT Benchmark Report by metagroup.com the projected growth of information technology's budget as percent of gross revenue for 2002 is flat or slightly negative. Also industries are cutting back even further from their 2001 IT spending (Table 1). [30]

However one positive note is that IT spending on computer security has increased since September 11, 2001. In November 2001, 67% of metagroup's respondents spent 0%-5% of their IT budget on security, and 33% spent 5% or more. According to metagroup this was a substantial increase from earlier in the year when 82% spent 0-5% on security, and only 18% spent more than 5%. [31]

Even though companies have increased spending in computer security, it does not mean that companies have accepted the national security plan versions

of corporate responsibility and security councils. In fact while there is an increase in security spending, at the same time the biggest cutbacks in information technology have been staffing. Also the number one priority in the United States and number two priority worldwide is reducing costs. [32]

Table 2: IT Spending

Industry	Average of IT Spending Change in dollars for 2001-2002
Information Technology	-22.22%
Electronics	-13.56%
Consumer Products	-12.19%
Financial Services	-10.94%
Construction and Engineering	-7.49%
Transportation	-7.28%
Energy	-5.47%
Telecommunications	-4.38%
Utilities	-4.00%
Media	-2.44%
Chemicals	-2.05%
Metals/Natural Resources	-1.31%
Manufacturing	-1.20%
Retail	-0.09%
Banking	-0.25%
Professional Services	1.32%
Food and Beverage	1.72%
Healthcare	2.62%
Insurance	3.39%
Pharmaceuticals	6.54%
Hospitality and Travel	10.04%
Overall	-3.08%

Source: Meta Group Inc., "2003 Worldwide IT Benchmark Report," (December 2002 accessed January 2003); available at http://www.metagroup.com/products/inforum/3_pdf/es_WB3.pdf; Internet.

Another part of the national security plan that corporations will not embrace is information sharing between the public and private sectors. Corporations would fear additional attacks, confidentiality problems, and

corporate espionage from competitors. That is like Coke giving its formula away to Pepsi. Corporations will not be a part of anything that will hurt their bottom line.

Global Preparedness

The global preparedness section of the national security plan is inadequate and does not reflect the current state of internet access worldwide. The plan calls for countries to pass cyber security laws so that the United States can investigate and prosecute cyber crimes against the United States and its interests. The first problem is that the only countries that have passed cyber crime legislation are the member countries of the European Union. This is good, but that region of the world is stable and not the primary concern of the United States.

As shown in Chapter 1 there is a rise in Internet usage in the troubled spots of the world that have shown at times to be an enemy of the United States. It is in these regions of the world that the problem lies. The authors of the national security plan expect these countries to draft and pass legislation to help the United States investigate and prosecute cyber crimes against the United States. These are the same countries that sponsor terrorism and cyber terrorism attacks against the United States.

The Patriot Act

In response to the September 11, 2001 terrorist attacks President George W. Bush signed into law on October 26, 2001 the Patriot Act (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism). The purpose of

the act is give law enforcement and intelligence officials greater authority to investigate people suspected of terrorist activity by monitoring telephone and Internet communications. The act also makes the DCS 1000 (Carnivore) system legal.

Carnivore is a high speed packet "sniffer" program developed by the FBI's Engineering Research Facility (ERIF) to conduct electronic surveillance of e-mail and Internet communications. Carnivore is installed at an Internet Service Provider's facility to monitor selected transmissions. [33]

According to the FBI, Carnivore works as follows: First, the FBI obtains a search order targeted to certain e-mail addresses or individuals. Then, the FBI and ISP identify an access point at the ISP that contains all traffic from the suspect. The FBI then connects a one-way tapping device at this access point, which produces an exact copy of all data at the access point. This data is then compared against a predetermined filter. Only data that is authorized for capture by court order passes through the filter and is stored on permanent storage media. [34]

Concerns of the Patriot Act

The passage of the Patriot Act brings into light a Fourth Amendment issue about unreasonable search and seizure. There is concern by many that the Patriot Act limits judicial oversight of electronic surveillance by: subjecting private Internet communications to a minimal standard of review, permitting law enforcement to obtain a "blank warrant," and authorizing intelligence wiretap

orders that do not specify the place to be searched or require that only the target's conversations be eavesdropped upon. [35]

When a judge authorizes a normal surveillance or search warrant, it specifies the place or area to be searched. If information seized from that place or area suggests that a search of another place is warranted, a law enforcement official must apply for a new warrant. The purpose of this process is to prevent unreasonable search and seizure and protect the privacy of individuals and due process. [36]

By contrast Section 216 of the Patriot Act permits a federal judge or magistrate to order to allow the FBI to installed Carnivore on an ISP's system. The order does not name the ISP's upon which it can be served. Rather law enforcement agents fill in the places at which the order can be served. [37]

According to the FBI, the Carnivore system is less intrusive than an ordinary telephone wiretap. Because the messages are in text format and the Carnivore "box" filters out content that cannot be seized pursuant to the court order, the FBI contends, a government agent does not screen every e-mail communication, but only those that are relevant to the investigation. However, in a typical wiretapping situation an agent listens in to every communication on the tapped telephone line to "filter" the relevant from the irrelevant conversations. Why should the Carnivore system be any different? [38]

When the FBI installs Carnivore on an ISP they are installing it on a network with many users who have no association with the party the FBI has under investigation. The information that Carnivore gathers is a combination of

the party under investigation as well as information about every user that is on the network. This is in contrast to a wiretap on a telephone line which is private, dedicated and only has one person assigned to that number.

On November 21, 2000, the Illinois Institute of Technology Research Institute released a 121 page report detailing its review of the Carnivore system. The report found that the program worked as advertised, but that "serious technical questions remain about the ability of Carnivore to satisfy its requirements for security, safety, and soundness." In stating that the "Carnivore system does not produce meaningful or secure audit trails," the reporters agree with the critics of Carnivore that "there are no adequate provisions for establishing individual accountability for actions taken during the use of Carnivore." [39]

Chapter 3 Summary

I have shown in Chapter 3 why the two policies concerning cyber terrorism will not protect the nation from a cyber attack. The first proposed policy, The National Strategy to Secure Cyberspace, looks at the problem, and tells the reader why the problem is a concern but does not provide a workable solution for every area. The current conflicts and the war on terrorism do not allow policy to be drafted without a solution. Answers to questions about how to combat cyber terrorism are needed now because the problem is real and it is only beginning.

The second policy, the Patriot Act, was passed into law. The bill was passed when the country was mourning the events of September 11, 2001 and

anyone that was against the act was viewed as unpatriotic. There was little debate and discussion and it was rushed through Congress before the members could fully understand the significance of the bill. This is why in chapter 4 I look at a way to amend parts of the Patriot Act so that it does not violate the First and Fourth Amendments to the United States Constitution.

CHAPTER 4

NATIONAL INFORMATION POLICY

The National Information Policy is a set of ideas brought together to combat the threat of a cyber terrorism attack against the infrastructures of the United States. The National Information Policy is based upon an outline by Wynn Schartwau in 1994. I have expanded on this outline and incorporated components into it that I believe are necessary to protect and defend the United States against a cyber attack.

Role of the Military

The organization that should be the center of the policy is the military. They should be the first line of defense if such an attack should occur. They have the resources, manpower, and the ability to organize for a quick response to a situation (Table 1). However, in order for this to occur, the military needs to expand its thinking from bombs, bullets, and physical warfare to computers, viruses, and information warfare.

There is no longer an immediate threat of foreign invasion using aircraft, ships, and other instruments of traditional warfare. However, there is an immediate threat of a cyber terrorist attack. As stated in Chapter 1, a cyber attack

can take seconds. Since September 11, 2001 the United States is a battlefield. No longer can the Atlantic and Pacific Oceans protect us from an attack. Homeland defense since September 11, 2001 has become critical to the national security of the United States.

Table 3: Number of Military and Civilian Personal

Force Type	Total	Force Type	Total
Army, Navy, Air Force, Marines	2,000,000	Coast Guard	48,000
National Guard	488,000	Federal Police	131,000
		State Police	55,000
		Local Police	650,000
	2,488,000		884,000

Source: John R. Brinkeroff, "The Changing of the Guard: Evolutionary Alternatives for America's National Guard.

The military can also take on another role of homeland defense and that is provide support to civilian authorizes in the case of a successful cyber terrorist attack. This concept is nothing new to the military. Since World War II the military has been used for peace keeping and humanitarian activities in certain parts of the world.

Posse Comitatus Law of 1878

The Posse Comitatus Law of 1878 ,however, prevents the military from taking an active role in law enforcement. The intent of the act is to prevent the military forces of the United States from becoming a national police force. The act specifically prohibits the military to "execute the laws." Execution of the laws is perceived to be a civilian police function, which includes the arrest and detention of criminal suspects, search and seizure activities, restriction of civilian movement through the use of checkpoints, gathering evidence for use in court,

and the use of undercover personnel in civilian, criminal, or drug enforcement activities.[1]

The problem with the law is that it was written in the nineteenth century when the threat to national security came from foreign governments with standing armies. Threats to national security have changed; today threats come from terrorists who do not practice traditional rules of warfare. For example the successful terrorist attacks on the Oklahoma City Federal Building and the World Trade Center showed that the homeland defense policy is inadequate. Local, state, and federal law enforcement agencies do not have the manpower and capabilities to prevent terrorist attacks.

The Framers of the Constitution opposed standing armies in general, for their use in any purpose other than defending the country against foreign armies. Two of the reasons for the American Revolution were the arrest of civilians by the British Army and the quartering of soldiers in private homes.

However terrorist attacks should not justify the United States in becoming a military state. A balance needs to be drawn between the roles of the military and civilian police. Congress needs to amend the Posse Comitatus Law so that the current threats to national security are meant.

The role of the military with the supporting intelligence agencies (National Security and the Central Intelligence Agency) should be to protect the nation's infrastructure against an attack, be in a ready state to respond to an attack with force against any aggressor nations, terrorist groups or individuals, and work closely with the civilian law enforcement agencies.

Cyberspace Boundaries

The military must first define the boundaries of the United States cyberspace. In order to do this, one must think in terms of a virtual world that intersects with the physical world. There are two types of cyberspace, a small and a big cyberspace, that when connected together create all of cyberspace.

The small cyberspace, known as "Little C," consists of private companies and government agencies. Private companies those such as Microsoft, Oracle, Amazon.com, Yahoo.com, and local Internet providers. Government agencies include the Department of Defense, Department of Energy, the Environmental Protection Agency, and state and local government offices. The big cyberspace, known as "Big C" consists of the six infrastructures (Chater 1, Table 1) that makeup the nation's infrastructures as a whole.

Information Conditions

The military needs to create Information Conditions (Infocons) so that each branch of the military and every government agency can follow them. The purpose of Infocons is to give the Information Technology System Administrator an indication of the current state of a cyber threat. They would also serve to provide a set of graduated actions to be taken in response to preestablished threat levels. This way once the protective measures have been breached, it is imperative that the breach is detected and assessed.

Given the current situation at the Department of Defense it is imperative that the military be the ones that establish the Information Conditions. Under the

current Department of Defense policy, most decisions about what countermeasures to apply and how to apply them are left in the hands of system administrators and other officials at individual Department of Defense facilities. The individuals lack guidance from the central command on how to apply countermeasures because countermeasures may affect a system's performance. Inexperienced personnel not trained in appropriate countermeasures may overreact and implement drastic countermeasures, resulting in self-inflicted problems, such as degraded system performance or communication disruption.[2]

Table 4: An Outline of Information Conditions

Infocon 5 – Normal peacetime readiness. Systems are up and running with security in place. Break-ins are attempted but failed.
Infocon 4 – A breaking attempt has been successful. The network has minimal damage and an investigation is under way.
Infocon 3 - The infrastructure security systems are heightened because of a physical attack or increased threat for a cyber attack.
Infocon 2 – A cyber attack has occurred on one or more infrastructures. The military is in a full state of readiness and preparing for a counter attack.
Infocon 1 – Systems meltdown. The nation's infrastructures have been attacked and temporarily disabled. A full-scale cyber war occurs.

Note: These information conditions are my own thoughts on how the dfferent stages of threat levels should be.

The "ILOVEYOU" virus showed why one entity such as the military should establish Information Conditions nationwide. When the "ILOVEYOU" virus struck at the Department of Defense widespread chaos occurred throughout the department. There was no uniformity and only poor communication between individual departments as to what was the appropriate Information Condition Level for responding to the cyber attack. Once the "ILOVEYOU" virus had emerged, it took the Department of Defense several hours to produce a

department wide recommendation on the appropriate Information Condition Level. Individual commands at the Department of Defense chose a variety of different levels and responses. The Information Condition System did not provide any specific guidance on the appropriate Information Condition Level or procedures for responding to the virus attack.[3]

Civilian Law Enforcement

Civilian law enforcement agencies are essential for prevention of a cyber terrorist attack. A team needs to be established made up of representatives from the Federal Bureau of Investigation, and state and local law enforcement officials. The team will be divided into zones based upon geographic regions of the country. The region will then send a representative to be a part of a committee, which would meet at the national level.

The objective of each team in the regions should be four fold: 1. intelligence gathering; 2. enforcement of computer laws including any laws that pertain to the Internet; 3. work with the private sector so that they are updated with the latest preventative measures; and 4. coordinate with the military in the event of an attack and a response to an attack.

For intelligence gathering the team should report how they will gather the information and what the information be used for. Once the information is collected the team should create profiles of the cyber terrorist personality that includes previous criminal activity, affiliations with criminal and/or terrorist organizations, e-mail addresses, handles, and known sites on the Internet that

the cyber terrorist visits on a regular basis. The information then needs to be stored in a database so that the information can be readily available to system administrators.

As part of information gathering, hackers should be considered as a valuable resource to the civilian law enforcement team. A lot of corporations already use hackers to identify weaknesses in their computer systems. The Legion of Doom, the most notorious hackers in the United States, formed a computer security business called Comsec Security.

The team needs to better enforce computer laws and laws pertaining to the Internet. The Computer Security Act of 1987 required federal agencies to identify systems that contain sensitive information and to develop a plan to safeguard them. Agencies were required to (1) identify all developmental and operational systems with sensitive information; (2) develop and submit to the National Security Agency for advice and commit a security and privacy plan for each system identified; and (3) establish computer security training programs. [4]

In 1990, the General Accounting Office examined the effectiveness of the act. Its report was alarming: only 38 percent of the 145 planned controls have been implemented. From this report alone one can conclude that there needs to be better enforcement of the computer security act. [5]

The civilian law enforcement agencies need to work with private sector companies so that the system administrators are aware of the latest vulnerabilities and what updates are needed for their systems.

A General Accounting Office report identified several factors of government and private organizations, which the organizations viewed as essential to establishing, developing, and maintaining effective information sharing relationships with other organizations, which could benefit critical infrastructure protection efforts. These factors included (1) fostering trust and rapport; (2) establishing effective, timely, and appropriately secure communication; (3) obtaining top management support; (4) ensuring organization leadership continuity; and (5) generating clearly identifiable membership benefits.[6]

Fostering trust and respect is an essential element for information-sharing organizations. Information technology executives should hold monthly meetings to establish face-to-face contact and discuss security issues. During this meeting time executives should develop personal relationships and contacts with other members. Each executive needs to participate in the discussion so that information could be shared properly and show that they could be trusted.

In order to establish effective, timely, and secure communications organizations need to have sectional meetings on a weekly basis. Regions, states or other sizes of organizations can break up into sections. Meetings need not always be held at a physical location, they can begin with physical or electronic face to face contact and then held by video or phone conference, and information can be posted on websites, in databases, and group chat sessions on the Internet.

IT executives should seek to obtain top management support so that they could share sensitive information about vulnerabilities in their company's computer network to the group. Without support from top management the IT executive contribution to the group would be limited.

The organization needs to ensure leadership continuity so that participation can be continuous, recruit new members, and keep current on issues and topics affecting their organization's membership.

The organization needs to have identifiable membership benefits to ensure growth in the organization. The benefits should include guaranteed access to current information about incidents, threats, and vulnerabilities that have been analyzed by trusted experts. Information about emerging technology, such as new software upgrades, so that they could be aware of possible vulnerabilities and the associated risks. A membership to the organization should entitle the executive to have free expert advice on individual projects. The executive should be aware of the opportunity to draw on a network of experts in order to give insight into their own problems and shortfalls in proposed projects. Members should receive real-time assistance in response to problems for other members of the organization and cooperation from law enforcement.

Corporations should not be afraid to report break-ins to their systems because of the fear of bad publicity or that competitors would gain an advantage. Computer based incidents such as the ILOVEYOU virus, the Code Red attack, and the denial of service attacks against Microsoft Hotmail and Morphesus have caused significant disruptions and damage. In addition, the terrorist attacks of

September 11, 2001 illustrate the importance of having timely information from others on threats and precursors to an attack.

For example if the Bank of America suffered an attack that crippled their online banking system most likely they would not make the information about the attack public for fear that people would stop using online banking or worse withdraw all their money and close their Bank of America accounts

However this is the wrong approach because other banking institutions such as Wells Fargo or US Bank are no more or less vulnerable to an attack. If the information about the attack was made public those two banking institutions can use the information to better secure their systems and protect their customers and their customers' assets.

Also if Bank of America goes public with information about the attack people might look at Bank of America as being an "honest banker."

Specific deterrence is a reason that companies should report an intrusion. When law enforcement catches and successfully prosecutes an intruder, that intruder is deterred from future assaults on the victim.[7] Law enforcement is also able to wiretap, pen/trap, trace orders, and enforce data preservation requests and other criminal process unavailable to a private party.

Restitution is also an attractive motive for victim reporting. A person must identify and repair damage and the costs can grow when the victim includes the loss of business and the loss of productivity of the technical staff dedicated to the intrusion. The company may be able to recoup some or all of the expenses through restitution. Reporting a criminal computer intrusion to law enforcement

may also help the victim recover under insurance policies for damage to its system or damage inflicted on a third party resulting from intrusion.[8]

Establishment of a Cyber Court

The passage of the Patriot Act in 2001 has caused great concern over violations of civil rights of individuals. A judicial component needs to be established in order to protect the civil rights of individuals and provide a check and balance system for law enforcement and government agency officials who are involved in investigations about cyber terrorism and cyber crimes.

Model of a Cyber Court

The cyber court would be modeled after the court established in the 1978 Foreign Intelligence Surveillance Act. It will oversee cases and investigations that are a "potential threat to the stability of society." It will be a seven-judge panel that would meet behind closed doors. This would allow law enforcement officials an opportunity to conduct investigations without the person(s) knowing he or she is under investigation. It would be the panel of judges responsibility to protect the integrity of the information and ensure there is no violation of civil rights.

The judges of the cyber court would also call upon the law enforcement officials and government agents to turn over all information that was gathered through the use of Carnivore for review. As discussed in chapter 3 it is the responsibility of the investigating official to filter through the relevant information and determine what information is necessary. Since all information is going to be gathered and stored by Carnivore in a database, something must be done with

gathered and stored by Carnivore in a database, something must be done with the irrelevant information so that it does not get misused or abused and an individual's right to privacy is protected.

The reason why the seven-judge panel has to meet in secret is because information travels at a rapid rate and can be either rerouted, changed, or deleted within seconds. By obtaining a warrant in confidence it would give law enforcement officials and government agents the ability to monitor the situation without the threat of exposure of their investigation.

Response to a Cyber Terrorist Attack

If an attack warrants a counter attack an outline must be drawn up by the military as to how to respond. The outline needs to include the identity of the military officials who will authorize a counter attack, definitions and roles and responsibilities of the military, the White House, and the intelligence communities; and identity high priority functions for maintaining national defenses including but not limited to national infrastructures and protecting the civilian population, rule of law, emergency preparedness, and the community of government.

Guidance of International Law

If a counter attack is necessary, it must be within the scope of international law and the United Nations Charter. The International Law of Conflict Management, "jus ad bellum," is a set of rules that govern the resort to armed conflict and determine whether the conflict is lawful or unlawful in its inception.[9]

Law of Conflict Management is central to understanding what is considered a use of force under international law because war is the legal consequence of a use of force by one state against another.

International law requires that all use of force be necessary and proportional, and it prohibits the use of force for retaliatory or punitive actions. The principles of necessity and proportionality apply under both the law of conflict management and the law of armed conflict. The law of armed conflict management requires that a state's use of force be necessary for either individual or collective self-defense. The law of conflict management requires that a state's use of force be proportional in intensity and magnitude to what is reasonably necessary to promptly secure the permissible objectives of self-defense.[10]

The principle of proportionality is a limitation on the use of force against a military objective only to the extent that such a use of force may cause unnecessary collateral destruction of civilian property or unnecessary human suffering of civilians. The principle of proportionality is a balancing of the need to attack a military objective with collateral damage and human suffering that will be caused to civilian property and civilians by the attack. However, it does not prohibit any damage to civilian property or injury to civilians. If civilian property and civilians support a war effort, they are subjected to attack, and they are subject to incidental damage during an attack on lawful military objective.[11] In relation to cyberspace, the nation has the right to respond to a cyber attack

against an individual or group because an attack on an infrastructure is considered an act of aggression that warrants an offensive reply.

While civilian property and civilians may not be the object of an attack, states may use force against civilian property and activities that support or sustain an enemy state's war fighting capability during armed conflict, for example against economic targets such as enemy lines of communication. Rail yards, bridges, rolling stock, bridges, industrial installations producing war fighting products, and power generation plants. In today's modern society, much of a state's civilian infrastructure is used for military purposes, and thus subject to lawful attack during armed conflict if there is a military advantage to be gained by such an attack.

> The Preamble of the Charter of the United Nations provides that one of the four goals is to ensure "that armed force shall not be used, save in the common interest..." to further this goal, all member states. Agreed in Article 2(3) that they "shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered." [12]

Accordingly, any state activity, which creates a dispute between two or more states, would violate the Article 2(3) proscription. Since these prohibitions apply to all potential state activities, any state activity in cyberspace that: (1) is an act of bad faith as it pertains to that state's dispute settlement negotiations, (2) otherwise threatens a peaceful settlement of that state's own dispute, (3) interferes with a dispute of other states in such a manner that would delay or prevent their dispute settlement, or (4) creates a dispute between states that

threatens international peace and security, violates a member states' obligations under Article 2(3)

> The right of self-defense may be invoked when a territorial state perceives a threat or use of force and has no alternative but to act to defend itself. Violations of international law may constitute a use of force within the meaning of Article 2(4) if they involve an exercise of power in the territorial domain of another state, even without the use of arms, but the response in self-defense must be necessary and proportional in view of the danger posed by the violation. For example, if a state enters the cyberspace boundary set by the United States military with the intent to cause damage, the United States has the right under Article 2(4) to take certain offensive measures. [13]

Recognizing that unarmed, non-military physical force by a state can affect another state just as severely as the use of armed military force, the Article 2(4) prohibition on the use of force also covers "physical force of a non-military nature" committed by any state agency.

It is also recognized that unarmed, non-military physical force "may produce the effects of an armed attack prompting the right of self-defense laid down Article 51."

This principle places far-reaching restrictions on a state's activities in Cyberspace that 'attack' the critical infrastructure of another state and cause destructive effects. A state can potentially cause significant property and economic damage, as well as human fatalities, in another state by utilizing the Internet.

Any destructive state activity intentionally caused within the sovereign territory of another state is an unlawful use of force. The cross-border use of weapons and bombardment of the territory of one state by another state is one of

the classic cases of a use of force within the meaning of Article 2(4). Accordingly, any state activity in Cyberspace that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force.[14]

Furthermore, even if such intentional destructive activities are an unlawful use of force that unequivocally invokes a victim state's right of self-defense, that right of self-defense does not necessarily justify a use of force in response. Similarly, not every destructive activity of this nature will reach the "intensity that enables them to be classified as 'armed attacks'." The scope, duration, and intensity of the force must be analyzed to determine if an armed attack has occurred.

The right to conduct espionage is an essential part of a state's inherent right of self-defense. The 1907 Hague Convention IV explicitly recognizes the lawfulness of espionage during armed conflict. Similarly, the 1961 Vienna Convention on Diplomatic Relations explicitly recognizes the well-established right of nations to engage in espionage during peacetime, and the practice of states has specifically recognized a right to engage in such clandestine intelligence collection activities as an inherent part of foreign relations and policy.[15]

The essence of espionage is the collection of information, and with the capabilities of today's inter-linked computers, there is perhaps no richer source of information than what can potentially be accessed via the Internet. What a state accesses information publicly available in databases in a foreign state, no unlawful act occurs under international or domestic law. Publicly available

information that has potential intelligence value is called open-source intelligence.

When one state hacks into another state's computer systems it is very likely engaging in acts that are unlawful under the domestic law of a territorial state, but under international law, the hacking state may be engaging in a lawful act of espionage that may not be considered a use of force.

But if a state has penetrated another state's information infrastructure to conduct espionage it is only one keystroke away from the capability of engaging in hostile and potentially destructive activities that are unlawful under international law.

The technology of computers and the Internet allows a lawful act of espionage to materialize into an unlawful use of force at the speed of light. Despite these practical problems, espionage conducted by the nonconsensual penetration of another state's computer systems is lawful under existing international law.

The right to respond in anticipatory self-defense does not apply to the penetration of all government computer systems during peacetime, but it should apply presumptively to those sensitive systems that are critical to a state's vital national interests.

For example, if a state accesses another state's computer systems such as early warning or command and control systems, missile defense computer systems, and other classified computer systems, such an act should by its very nature be presumed a demonstration of hostile intent.

Chapter 4 Summary

Chapter 4 I laid out my proposal for a National Information Policy. I believe this policy would be the most aggressive steps the United States needs to take to combat a cyber terrorist attack. The National Information Policy is a foundation that can be built upon for years to come since the ground work of who will be in charge of what and how to go about achieving objectives would have already been set.

The National Information Policy with the establishment of the Cyber Court overturns the mistakes that were made with the passage of the Patriot Act. As we go deeper into the Information Age we must not forgot the fundamentals written in the Bill of Rights on which the United States was founded.

CHAPTER 5

CONCLUSION

The invention of computers has been coined as the "Second Industrial Revolution." Computers have given society the ability to perform their daily functions with ease. However with every great invention comes a dark side, with the invention of computers it is cyber terrorism.

The infrastructure of the United States is dependent upon computers and within seconds the infrastructure can collapse from a cyber terrorist attack. It takes a cyber terrorist seconds to break into a computer and create mass destruction without ever being detected. It is vital that the United States adapt the National Information Policy as a foundation for combating the cyber terrorist threat.

A cyber terrorist is the type of person who has a low self-esteem and is an outcast from society. He or she will do anything to acquire fame, fortune, and acceptance. This type of person is extremely dangerous and they must be prevented at all costs.

The recent policies by the United States to combat the threat of cyber terrorism are not sufficient. The "National Strategy to Secure Cyber Space" explains what the problem is but does not give a solution to the problem. The

"Patriot Act" is a law that is in violation of the First and Fourth Amendments of the United States which were drafted to protect an individual's civil liberties

I believe the National Information Policy is the best policy to maintain control of the information. The United States on September 11, 2001 become a battlefield. The redefined role of the military protects the United States from nations, groups, and individuals who do not practice rules of traditional warfare. The cooperation between the public and private sectors ensures there will be continuous communication between all parties involved in protecting the United States from a cyber terrorist attack. Finally, the establishment of a cyber court guarantees that an individual's civil liberties are not being violated by law enforcement officials when conducting an investigation.

Cyber terrorism is the new type of warfare. The attacks will become more frequent and cause more destruction. Information control is the single most important resource of a country, since whoever controls the information also has the power. With the rise of Internet usage outside North America, it is more important to keep control of that information and keep the information out of the hands of criminal and terrorist organizations and nation states that are anti-US.

In conclusion, cyber terrorism is the new type of threat that the United States faces in the coming years. It is the type of threat that needs immediate solution since an attack can happen anywhere and at anytime. Cyber terrorism affects everyone therefore it is everyone's responsibility to combat the threat.

ENDNOTES

Chapter One

1. "The Clinton Administration Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," (May 22, 1998, accessed 23 November 2002); available from http://www.nipc.gov/about/pdd63.htm; Internet.

2. Scarlett Pruitt, "16 Agencies Flunk Computer Security Review," Computerworld, November 9, 2001; http://www.computerworld.com/security/Story/0,10801,65589,00.html; Internet; accessed 18 January 2002

3. "The Online Population," (July 2001, accessed 8 September 2001); available from http://www.idc.com/en_US/browse/viewBrowseRes.jhtml; Internet.

4. United States Internet Council & ITTA Inc. "State of Internet 2000" (March 2001, accessed May 2001); available from http://usic.wslogic.com/intro.html; Internet.

5. United States Internet Council & ITTA Inc. "State of Internet 2000" (March 2001, accessed May 2001); available from http://usic.wslogic.com/intro.html; Internet.

6. Cyberatlas Staff. "The World's Online Populations" (March 2002, accessed July 2002); available from http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_151151,00.html; Internet.

7. United States Internet Council & ITTA Inc. "State of Internet 2000" (March 2001, accessed May 2001); available from http://usic.wslogic.com/intro.html; Internet.

8. Angus Reid Group, "The Face of the Web" (April 2001, accessed April 2001); available from http://www.angusreid.com/us/services/dsp_little_net_book.cfm#raw; Interne

9. Cyberatlas Staff. "China's Online Population" (November 2002, accessed December 2002); available from http://cyberatlas.internet.com/big_picture/geographics/article/0,5921_1013841,00.html; Internet.

10. Cyberatlas Staff. "More Russians Get Online" (May 2002, accessed July 2002); available from http://cyberatlas.internet.com/big_picture/geographics/article/0,5521_113641,00.html; Internet.

11. Cyberatlas Staff. "More Russians Get Online" (May 2002, accessed July 2002); available from http://cyberatlas.internet.com/big_picture/geographics/article/0,5521_113641,00.html; Internet.

12. "Internet Population Explodes in the Middle East," The Information & Technology Company, March 2001, 6. These figures do not include the nation of Israel.

13. "Internet Population Explodes in the Middle East," The Information & Technology Company, March 2001, 6. These figures do not include the nation of Israel.

14. Cyberatlas Staff. "The World's Online Populations" (March 2002, accessed July 2002); available from http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_151151,00.html; Internet.
The 38.3% for the UAE and the 38.92% for the US are based upon the total number of Internet users fort each country.

15. The White House, "National Strategy to Secure Cyberspace," September 2002, prepared by Presidents Critical Infrastructure Protection Board, The White House [Cd-Rom], page 5.

16. Michael A. Vatis, "Cyber Attacks During the War on Terrorism: a predicative analysis" (paper, Institute for Security Technology Studies at Darmouth College, September 2001).

17. Stanley A. Miller, "Data Protections on Internet May Have Helped Plotters," Milwaukee Journal Sentinel, (September 16, 2001 accessed September 16, 2001); available from http://www.jsonline.com/; Internet.

18. Ibid.

Chapter Two

1. Nicholas Chantler, "Profile of a Computer Hacker" (Ph.D. diss., University of Queensland, 1996), 3-4.
2. Ibid.

3. Michele Slatalla, "A Brief History of Hacking," The Learning Channel (December 2001 accessed January 2002); available from http://tlc.discovery.com/convergence/hackers/articles/history.html; Internet.

4. Ibid.

5. Ibid.

6. Ibid.

7. Nicholas Chantler, "Profile of a Computer Hacker" (Ph.D. diss., University of Queensland, 1996), 6.

8. Ibid., 7.

9. Ibid., 9.

10. Ibid., 10.

11. Jeremy Quittner, "Hacker Psych 101," The Learning Channel (December 2001 accessed January 2002); available from http://tlc.discovery.com/convergence/hackers/articles/psych.html; Internet.

12. Rex A. Hudson, "The Sociology and Psychology of Terrorism: Who Becomes and Why?" Federal Research Division (September 1999 accessed February 2003); available from http://www.loc.gov/rr/frd/Sociology-Psychology%20of%20Terrorism.htm; Internet.

13. Ibid.

14. Ibid.

15. Ibid.

16. Dorthory Denning, Information Warfare and Security (New York: Pearson Education, 1998), 34.

17. Ibid.

18. Roger W. Barnett, "Information Operations, Deterrance, and the Use of Force" (Spring 1998 accessed April 2001); available from http://www.nwc.navy.mil/press/review/1998/spring/art1-sp8.htm; Internet

19. Ibid.

20. Ibid.

21. Lt. Col Fredrick Okelo, Major Richard Ayers, Major Patrice Bullock, Major Brahim Erhili, Major Bruce Harding, and Major Allan Perdigao, "Information Warfare: Planning the Campaign" (Research paper, Air Command and Staff College, 1996), 40.

22. Ibid., 42.

23. Ibid., 45.

24. Ibid., 46.

25. Ibid., 47.

26. Ibid., 51.

27. Ibid., 51.

28. Ibid., 54.

29. Ibid., 58.

30. Ibid., 60.

31. Ibid., 61.

32. Ibid., 63.

33. Ibid., 65-66.

34. Ibid., 66.

35. Ibid., 68.

36. Ibid., 69.

Chapter Three

1. The White House, "National Strategy to Secure Cyberspace," September 2002, prepared by Presidents Critical Infrastructure Protection Board, The White House [Cd-Rom], page 7.

2. Ibid., 8.

3. Ibid., 11.

4. Ibid., 15.
5. Ibid., 16.
6. Ibid., 16.
7. Ibid., 16.
8. Ibid., 16.
9. Ibid., 16.
10. Ibid., 19.
11. Ibid., 19.
12. Ibid., 20.
13. Ibid., 20.
14. Ibid., 23.
15. Ibid., 24.
16. Ibid., 25.
17. Ibid., 25.
18. Ibid., 25.
19. Ibid., 25.
20. Ibid., 25.
21. Ibid., 27-28.
22. Ibid., 29.
23. Ibid., 29.
24. Ibid., 31.
25. Ibid., 31.
26. Ibid., 35.

27. Ibid., 35.

28. Ibid., 49.

29. Ibid., 50.

30. Meta Group Inc., "2003 Worldwide IT Benchmark Report," (December 2002 accessed January 2003); available at http://www.metagroup.com/products/inforum/3_pdf/es_WB3.pdf; Internet, page 2.

31. Ibid., 3.

32. Ibid., 5.

33. Margaret Smith Kubiszyn, "Legal Controversy and the FBI's Carnivore Program," Gigalaw.com, (December 2000 accessed December 2002); available at http://www.gigalaw.com/articles/2000-all/kubiszyn-2000-12a-all.html; Internet.

34. Ibid.

35. ACLU, "How the Patriot Act Limits Judicial Oversight of Telephone and Internet Surveillance," The American Civil Liberties Union, (October 2001 accessed January 2002); available at http://archive.aclu.org/congress/l102301g.html; Internet.

36. Ibid.

37. Ibid.

38. Margaret Smith Kubiszyn, "Legal Controversy and the FBI's Carnivore Program," Gigalaw.com, (December 2000 accessed December 2002); available at http://www.gigalaw.com/articles/2000-all/kubiszyn-2000-12a-all.html; Internet.

39. Ibid.

Chapter Four

1. "The Posse Comitatus Act: A Principle in Need of Renewal," Washington University Law Quarterly (Summer 1997 accessed July 2002); available at http://law.wustl.edu/WULQ/75-2/752-10.html; Internet.

2. U.S. Congress. Senate. 2001. "Information Sharing: Practices That Can Benefit Critical Infrastructure Protection." Washington, D.C.: GAO.

3. Ibid.

4. Ibid.

5. Ibid.

6. Ibid.

7. Richard P. Salgado, "Working with Victims of Computer Network Hacks," United States Attorneys' USA Bulletin (March 2001 accessed July 2002); available at http://www.usdoj.gov/criminal/cybercrime/usamarch2001_6.htm; Internet.

8. Ibid.

9. Michael Erbschle and John R. Vacca, How to Survive Cyber Attacks (New York: McGraw-Hill Professional, 2001), 187.

10 Ibid., 190.

11. Ibid., 190-191.

12. Ibid., 194.

13. Ibid., 195.

14. Ibid., 197.

15. Ibid., 198.

APPENDIX I

April 24, 2003

Dear Mr. Nicholas Chantler,

I am writing this letter to inform you that I will be using a figure from your dissertation "Profile of a Computer Hacker." The figure is titled "The Birth of a Hacker – A Conceptualisation based on the Literature" and can be found on page 37 in your dissertation.

Sincerely,

Daniel A. Nick

APPENDIX II

April 24, 2003

Dear Ms. Dorothy Denning,

I am writing this letter to inform you that I will be using a figure from your book Information Warfare and Security. The figure is a diagram of an information warfare operation and can be found on page 24 in your book.

Sincerely,

Daniel A. Nick

BIBLIOGRAPHY

ACLU "How the Patriot Act Limits Judicial Oversight of Telephone and Internet Surveillance," The American Civil Liberties Union. October 2001 accessed January 2002; available at http://archive.aclu.org/congress/l102301g.html; Internet.

Angus Reid Group. "The Face of the Web" April 2001, accessed April 2001; available from http://www.angusreid.com/us/services/dsp_little_net_book.cfm#raw; Internet.

Barnett, Roger W.. "Information Operations, Deterrance, and the Use of Force." Spring 1998 accessed April 2001; available from http://www.nwc.navy.mil/press/review/1998/spring/art1-sp8.htm; Internet.

Chantler, Nicholas. "Profile of a Computer Hacker." Ph.D. diss., University of Queensland, 1996.

"The Clinton Administration Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." May 22, 1998, accessed 23 November 2002; available from http://www.nipc.gov/about/pdd63.htm; Internet.

Cyberatlas Staff. "China's Online Population." November 2002, accessed December 2002; available from http://cyberatlas.internet.com/big_picture/geographics/article/0,5921_1013841,00.html; Internet.

Cyberatlas Staff. "More Russians Get Online." May 2002, accessed July 2002; available from http://cyberatlas.internet.com/big_picture/geographics/article/0,5521_113641,00.html; Internet.

Cyberatlas Staff. "The World's Online Populations." March 2002, accessed July 2002; available from http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_151151,00.html; Internet.

Denning, Dorothy. Information Warfare and Security. New York: ACM Press, 1999.

Erbschle, Michael and John R. Vacca. How to Survive Cyber Attacks. New York: McGraw-Hill Professional, 2001.

"Internet Population Explodes in the Middle East." The Information & Technology Company. March 2001.

Kubiszyn, Margaret Smith. "Legal Controversy and the FBI's Carnivore Program." Gigalaw.com. December 2000 accessed December 2002; available at http://www.gigalaw.com/articles/2000-all/kubiszyn-2000-12a-all.html; Internet.

Meta Group Inc. "2003 Worldwide IT Benchmark Report." December 2002 accessed January 2003; available at http://www.metagroup.com/products/inforum/3_pdf/es_WB3.pdf; Internet.

Miller, Stanley A. "Data Protections on Internet May Have Helped Plotters." Milwaukee Journal Sentinel. September 16, 2001 accessed September 16, 2001; available from http://www.jsonline.com/; Internet.

Oilelo, Fredrick Lt.Col, Major Richard Ayers, Major Patrice Bullock, Major Brahim Erhili, Major Bruce Harding, and Major Allan Perdigao. "Information Warfare: Planning the Campaign." Research paper, Air Command and Staff College, 1996.

"The Online Population." July 2001, accessed 8 September 2001; available from http://www.idc.com/en_US/browse/viewBrowseRes.jhtml; Internet.

Pruitt, Scarlett. "16 Agencies Flunk Computer Security Review." Computerworld. November 9, 2001, accessed 18 January 2002; available from http://www.computerworld.com/security/Story/0,10801,65589,00.html; Internet.

"The Posse Comitatus Act: A Principle in Need of Renewal." Washington University Law Quarterly. Summer 1997 accessed July 2002; available at http://law.wustl.edu/WULQ/75-2/752-10.html; Internet.

Quittner, Jeremy. "Hacker Psych 101." The Learning Channel. December 2001 accessed January 2002; available from http://tlc.discovery.com/convergence/hackers/articles/psych.html; Internet.

Salgado, Richard P. "Working with Victims of Computer Network Hacks." United States Attorneys' USA Bulletin. March 2001 accessed July 2002; available at http://www.usdoj.gov/criminal/cybercrime/usamarch2001_6.htm; Internet.

Schwartau, Winn. Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age. New York: Thunder's Mouth Press, 1996.

Statalla, Michele. "A Brief History of Hacking." The Learning Channel. December 2001 accessed January 2002; available from http://tlc.discovery.com/convergence/hackers/articles/history.html; Internet.

United States Congress. Senate. 2001. "Information Sharing: Practices That Can Benefit Critical Infrastructure Protection." Washington, D.C.: GAO.

United States Internet Council & ITTA Inc. "State of Internet 2000." March 2001, accessed May 2001; available from http://usic.wslogic.com/intro.html; Internet.

Vatis, Michael A. "Cyber Attacks During the War on Terrorism: a predicative analysis." paper, Institute for Security Technology Studies at Darmouth College, September 2001.

The White House "National Strategy to Secure Cyberspace." September 2002, prepared by Presidents Critical Infrastructure Protection Board, The White House [Cd-Rom].

VITA

Graduate College
University of Nevada, Las Vegas

Daniel A. Nick

Local Address:
1605 Crimson Hills #103
Las Vegas, Nevada 89128

Degrees:
Bachelor of Arts, History 1994
Gannon University

Thesis Title: The Creation of a National Information Policy Combating Cyber Terrorism

Thesis Examination Committee:
Chairperson, Dr. Alan Zundel, Ph.D.
Committee Member, Dr. Craig Walton, Ph.D.
Committee Member, Dr. Karen Layne, Ph.D.
Graduate Faculty Representative, Dr. Kendall Hartley, Ph.D.