# THE DIGITAL THREAT:
## UNITED STATES NATIONAL SECURITY AND COMPUTERS

Matthew G. Devost
Department of Political Science, University of Vermont, Burlington, VT 05401

COMMENTS WELCOME

---

Paper prepared for Presentation at the 1994 Annual Meeting of the New England Political Science Association, Hawthorne Hotel, Salem, Massachusetts, April 24, 1994.

## Abstract:

This paper examines the effects of computer technology on United States infrastructure, especially in areas of national security. It examines what vulnerabilities new technology has created, how those vulnerabilities have been exploited in the past, and how the United States has reacted to problems that have arisen out of computer technology. In the United States, computer technology controls many aspects of our daily lives including communications, finances, health, transportation, and our national security. Recent proposals by Vice President Gore to create an "Information Superhighway" only promise to increase our reliance on these computer systems. Very little public debate has arisen over which direction this technology is taking us, what vulnerabilities it creates, and what price on individual privacy will be imposed when eradicating these vulnerabilities.

This paper serves as an introduction to the issues that have arisen out of this new technology, as well as providing suggestions for future public policy concerns. It examines the inherent weaknesses of such systems by studying several cases in which United States national security has been in jeopardy, and how the United States has responded to these problems. It ends with an evaluation of current legislation and political posturing on technological issues and concludes with several policy prescriptions that would smoothen the United States entrance into the digital age.

## The Digital Revolution

> **"The medium, or process, of our time - electronic technology - is reshaping and restructuring patterns of social interdependence and every aspect of our personal life. It is forcing us to reconsider and re-evaluate practically every thought, every action, and every institution formerly taken for granted."[1]**

When researchers at the U.S. Defense Department Advanced Research Projects Agency (ARPA) began linking computers together in the hopes of establishing a network to share data that would survive a nuclear attack, they never imagined that their labor would result in the worldwide network known as the Internet. The Internet, commonly referred to as the Information Superhighway, now connects millions of computers and is growing at exponential rates. Access to the Internet was originally limited to large universities and military bases, but new technology enables millions of people using personal home computers to access the Internet through telephone lines.

One of the most well known aspects of the Internet is Electronic Mail or e-mail. E-mail allows a user at one site to send electronic messages to any other site in the world. The message usually arrives at its destination in less than an hour. The ability to log onto a machine thousands of miles away in order to run programs is another basic capability of the Internet. This is accomplished using the Telnet command which connects the user with the remote machine. However, a valid account or permission to use the remote machine is required otherwise access is denied.

Another Internet utility, the File Transfer Protocol (ftp) allows users to log onto remote machines and obtain files at very fast speeds, allowing the retrieval of large files like the entire Encyclopedia Britannica from across the country in just one or two seconds[2]

Access to networking capabilities has already created a new industry. There are companies that have created points of access to the Internet and market this service to the general public for a fee.

## The Digital Threat

These networked computer systems share one common interface: information. There are three categories of information on the Internet: (1) military information, which deals with actual military developments, top secret operations, intelligence, systems control, correspondence between high ranking officials, troop files, credit ratings, general troop activities and lower level correspondence; (2) business information which consists of business records, bank transactions, individual credit records, business systems, and Wall Street transactions; (3) personal information which includes personal systems, files and correspondence between individuals.

An attack or threat on lower levels of information is more of an inconvenience than a national security threat. Replacement costs may be high for this type of information, but the costs are not nearly as high as military or business information. A successful attack on just a few business information systems could cause a severe lag in the American economy. Robert Steele notes that "It costs a billion dollars and takes six weeks to recover from a one day bank failure and we have them all the time."[3] If Wall Street suddenly closed down, or if bank transactions suddenly disappeared the United States would lose hundreds of billions of dollars. A potential attack on military information, especially that which is classified, poses a national threat from a strategic standpoint. What if, during a war, the enemy was able to get information on troop movements or discover flaws in one of our weapons systems? Or if the Soviet's had been able to access information on the Strategic Defense Initiative during the Cold War? What if one fourth of all the computer systems in America stopped working one day?

## The Hacker Threat

Who has the capability to attack such systems and how do they keep from getting caught? The computer hacker was originally someone who spent years creating and exploring the new technology of computer networks. Today the term hacker has come to mean two different things. Once they were computer enthusiasts with an urge to learn more about the inner workings of the technology. When their predictions about where the industry was headed came true, some of them eventually became rich. As these original hackers created a community on the electronic frontier they realized the value of their creations and decided that access to information should cost money. Eventually they saw the need to secure the product of their labor.[4] Security became a concept applicable to computer systems and the information they contain. Walls went up, password protection became a standard and certain areas were placed off limits to a large portion of the computer community. Thus, the second generation of hackers were greeted with locked doors and forced to explore the inner workings of computer systems covertly, like underground explorers of a resource-rich cave. They became skilled manipulators of information systems, but they never abused them, nor did they use their skills for illegal means. However, along with this second generation of hackers arose a new breed who chose to use technology for their own benefit. The media does not distinguish between curious second generation hackers and this new breed. These new hackers see information as a power force all its own that longs to be free. They often liberate it by illegal means, copying information files they are not supposed to have then using these files as a commodity to trade for more information. This is the digital underground and "forbidden knowledge is their basic currency."[5] In the digital world where the digital underground exists, the distinction between crime and curiosity becomes blurred, and only society can decide where to draw the line between the two.

The members of the digital underground are good at what they do, and their skills are available to outside parties for a price. They assume aliases and congregate on

underground systems around the world, bragging about their hacker prowess and sharing information with each other. Often they are motivated by personal greed or pride. Sometimes they are motivated by anger or ideology, striking at the system, the big corporations, or each other. They form groups and gangs like the Legion of Doom and the German Chaos Computer Club. Most of them are alienated individuals, intelligent kids labeled as underachievers. Their only friends are this new found technology and the people who are as interested in it as they are. A hacker named Mentor describes his experience in the world of the digital underground:

> I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me....And then it happened...a door opened to a world...rushing through the phone line like heroin through an addicts veins, and electronic pulse is sent out, a refuge from day-to-day incompetencies is sought...a board is found. This is it...this is where I belong...I know everyone here...even if I've never met them, may never hear from them again...I know you all...This is our world now...the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore...and you call us criminals. We seek after knowledge...and you call us criminals. We exist without skin color, without nationality, without religious bias...and you call us criminals. You build atomic weapons, you wage wars, you murder, cheat and lie to us and try to make believe that it's for our own good, yet we're the criminals. Yes I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something you will never forgive me for.[6]

This digital underground exists with an inclination against the system, mostly because the system categorizes them as criminals for doing something they love. Those in the digital underground like to demonstrate the position of power from which they operate. They do in fact outsmart the system every day, by gaining access to the systems they want, often for free. They are not inclined to do damage unless provoked or offered something in exchange like recognition or money. Mostly, they are just curious, rebellious teenagers caught in the digital age. They use the system to show their power; they demand respect. If you don't give it to them, they will scare it out of you by demonstrating their capabilities. A few years ago, Harpers magazine hosted an electronic forum to discuss the legality of

computer hacking. It attracted a diversified array of individuals including privacy advocates, hackers and computer security professionals. Two of the participants in the forum, John Perry Barlow (ex lyricist for the Grateful Dead) and Phiber Optik (a young hacker) became engaged in debate during which Barlow referred to hackers as an offbreed of skateboarders. An inferiorated Phiber Optik left the forum and ten minutes later responded to Barlow's accusation by uploading a complete listing of Barlow's credit history. Barlow said of the incident: "I've been in redneck bars wearing shoulder length curls, police custody while on acid, and Harlem after midnight, but no one has ever put the spook in me quite as that Phiber Optik did at that moment. To a middle-class American, one's credit rating has become nearly identical to his freedom."[7] It is essential that we recognize the motives of the hackers in order to offer a better understanding of their intentions. They are looking for a place to play and learn. That place exists on the wires, off limits. So they take without asking. While their curiosity does not pose an immediate threat to our society, it has potential. The KGB found someone with that potential in Germany just a few years back.

## The Hacker Spy

Perhaps the best publicized account of a hacker breaking into U.S. military computer systems took place in 1986 when Cliff Stoll at the Lawrence Berkeley Laboratory (LBL) discovered a German hacker using the university's computer to access sensitive databases. Stoll's adventure began when he found a seventy-five cent error in the LBL accounting system that tracks system usage and then bills the correct party. By exploring the accounting software, Stoll found that a user named Hunter had used seventy-five cents worth of computing time in the last month. Stoll also discovered that Hunter did not have a valid billing address, so he had not been properly charged. Through much work, Stoll discovered that Hunter was in fact a computer intruder, a hacker using LBL's system to access other systems. In most cases the user would have been shut out, but Stoll an

astronomer by trade, not a computer security expert, decided to try and track the activity of the hacker.[8]

When Stoll first discovered that the hacker was accessing military computers, no one believed him. The people in charge of maintaining these sensitive systems did not know, nor did they believe that a hacker had entered their system. Stoll had a even harder time trying to convince law enforcement agencies that this was indeed a crime worthy of having the hacker's call traced. This one hacker attempted to break into many military computer installations including the Redstone Missile Command in Alabama, the Jet Propulsion Laboratory in Pasadena, and the Anniston Army Depot. In many of the cases the hacker successfully gained full access of the system and searched for keywords like stealth, nuclear,. White Sands and SDI.[9] When he found the files he copied them to his home computer.

The search for the hacker continued for almost a year, and the activity was eventually traced to a West German citizen named Markus Hess. Hess, a member of the hacker group called the German Chaos Computer Club, used the pseudonym Pengo among his colleagues and was known as one of the best hackers in the Hannover area. On February 15, 1990, Hess and two colleagues were convicted of espionage for selling secrets to the KGB.[10]

Surely one must look at this case as a threat to U.S. national security, especially in the context of the Cold War. Gone are the days of searching for Ivans in elite factions of the U.S. military. Now any twenty year old German drug addict can accomplish the same thing from an apartment in West Germany. The networking of computers gives him the means, and the lax security of the United States in protecting their computer systems allows him to compromise U.S. national security. The United States learned a lesson from this experience and responded to this possible threat with legislation.

## The Computer Security Act

The United States Congress passed a law titled the Computer Security Act of 1987 which required federal agencies to identify systems that contain sensitive information and to develop plans to safeguard them. Agencies were required to (1) identify all developmental and operational systems with sensitive information, (2) develop and submit to NIST and NSA for advice and comment a security and privacy plan for each system identified, and (3) establish computer security training programs.

Finally, the United States was taking the threat of national security posed by computer access seriously. The Computer Security Act was a step in the right direction, but holes still exist. In 1990, the General Accounting Office examined the response and implementation of the act. The GAO reports that as of January 1990, only 38 percent of the 145 planned controls had been implemented.[11] The GAO report makes the following conclusion:

> **The government faces new levels of risk in information security because of increased use of networks and computer literacy and a greater dependence on information technology overall. As a result, effective computer security programs are more critical than ever in safeguarding the systems that provide essential government services.[12]**

With only a 38 percent compliance more needs to be done if the United States is to seriously protect its valuable informational assets. Instead of concentrating on making the systems more secure, the government chose to focus on the intruders of these systems. Time, energy and money that should have been spent discovering and fixing security bugs was instead used to design and implement an attack on the hackers themselves. This was an attack that focused only on domestic hackers and did little to thwart the threat to United States national security. The result: Operation Sundevil.

## Operation Sundevil

Law enforcement agencies had already begun to focus their attack on the digital underground when Operation Sundevil was initiated, but it was by far the largest clamp down on computer crime in the United States. The focus of Operation Sundevil was the hackers' system of information distribution which consisted of hundreds of underground computer systems that housed information on how to break into computer systems, files stolen from major U.S. corporations, and files that contained credit card access numbers used to commit credit fraud. Around forty-two computers were seized along with 23,000 floppy disks of information during the May 7, 8, and 9, 1990 raids.[13]

Across the United States teenagers and their parents awoke to Secret Service revolvers pointed at their heads, followed shortly by a search of their house and the confiscation of anything that looked remotely electronic. Misinformation led to a few mistakes as well. Perhaps the most publicized of these was the raid on Steve Jackson Games. Jackson owned a small company that ran a bulletin board system that allowed his game players to call in and ask questions, arrange meetings, etc. Jackson also unknowingly employed a computer hacker. The Secret Service tied the two together and as a result Steve Jackson Games was raided and all their computer equipment was seized and never returned. This greatly effected Jackson's business and he nearly went bankrupt. Jackson recently won a law suit against the Secret Service in the amount of $52,000 plus legal fees.[14]

The United States has a vested interest in preventing computer crime and fraud, and Operation Sundevil was surely a huge attack on such crimes, but it was greatly misdirected. While teenage hackers were arrested and tried, U.S. military systems and business systems remained open to attack. Hackers will always exist and the only true way to stop them is to plug the holes they use to gain access to systems. The solution lies not in ignoring domestic computer crime, but in giving a higher priority to increasing computer security. During the Gulf War, that lesson would prove true again.

## Hacker Attacks During the Gulf War

The United States inability to protect its computer systems was reinforced by attacks on Department of Defense computer systems during the war with Iraq. Testimony before a Senate committee confirmed that between April and May of 1991, computer hackers from the Netherlands penetrated 34 Department of Defense computer sites. Here are few highlights from the report.

> **At many of the sites, the hackers had access to unclassified, sensitive information on such topics as (1) military personnel--personnel performance reports, travel information, and personal reductions; (2) logistics - descriptions of the type and quantity of equipment being moved; and (3) weapons system development data. Although the information is unclassified, it can be highly sensitive, particularly during times of international conflict. For example, information from at least one system, which was successfully penetrated at several sites, directly supported Operation Desert Storm/Shield. In addition, according to one DOD official, personnel information can be used to target employees who may be willing to sell classified information.[15]**

It is highly disturbing that U.S. soldiers put their lives on the line to fight a war for a country that cannot even protect the sensitive information related to their activities, let alone personal data that could be used against their families. What is most distressing about the reports is its conclusion that the hackers exploited known security holes to gain access to a majority of these systems. The United States government knew that these security holes were there, yet it did nothing to fix them. The report also indicates that the hackers "modified and copied military information"[16],and concluded that many of the sites were warned of their vulnerability but failed to realize the implications. The report ended with a warning of things to come: "Without the proper resources and attention, these weaknesses will continue to exist and be exploited, thus undermining the integrity and confidentiality of government information."[17]

Limited research in the media coverage of this event did lead to one source who reported what had happened, Geraldo Rivera. The national security of our nation is at stake and it takes Geraldo to inform the public. It would appear that the United States would prefer that the public not know about such weaknesses. Big businesses, too, have a

vested interest in keeping such attacks on their systems secret. After all, who wants to put their money in a bank, when they know that one day it may disappear due to computer vulnerability? It is like asking people to put their money in a bank that doesn't lock its door at night.

So far, this essay has only touched upon one aspect of computer vulnerability: computer intrusion. The second form of computer vulnerability to be examined here deals with programmed attacks on computer systems with the intent to do as much damage as possible. This is the world of the computer virus, trojan horse and worm.

## Virii, Trojan Horses and Worms

Virii, trojan horses and worms have huge destructive potential. Perhaps the greatest threat of the three is the computer virus, a program which has the ability to attach itself to legitimate files and then propagate, spreading much like an infectious disease from computer to computer as files are exchanged between them. The more interactivity your computer has with other computers the higher the chance of it contracting a virus. The virus continues to hide itself until a certain criteria is met. These criteria change from virus to virus, but some of the most deadly are virii that wait a certain length of time before initiating their destructive capabilities. This insures that the virus has had enough time to copy itself to many systems, thus increasing its damage potential. Once the criteria are met, the virus attacks your system in one of many ways: by erasing files, destroying hard disk drives, or corrupting databases.

Imagine a virus that spreads to a bank computer and then randomly modifies numbers within the database, or simply causes the bank's computers to shut down. The potential for damage is enormous, but it is mostly monetary damage. Now imagine that same virus attacks a hospital computer system. Human lives are at stake, making that virus a tool of murder no less dangerous than a loaded weapon. Virii are very difficult to protect against because a copy of the virus is often needed to create a vaccine or program to detect

it. We do not usually find copies of the virus until they have caused damage. It has been estimated the cost of removing the virii infections over the next five years will be over $1.5 billion - not taking into account the value of the data that will be destroyed.[18] There are already many documented cases of companies losing millions of dollars in business and thousands of hours of computing time due to virii attacks.[19] That number will only increase in the future.

By 1992 there were over 1,500 catalogued viruses in the West, with that number expected to have doubled by the end of 1993[20] One of the most popular was the Michaelangelo virus that received news coverage on all the major networks. What many Americans don't understand is that Michaelangelo is just one of many potential attackers of their computer systems. In Bulgaria, companies have set up virus factories producing more virii than the anti-virus industry can combat. How should the U.S. deal with such companies whose only concern is to produce destructive software? This is one of the many questions we must ask ourselves when creating policies to ensure safe computing in future years.

The trojan horse derives its name from the famous attack on the city of Troy, and operates much like the trojan horse of ancient times. A trojan horse is a program that pretends to be something else but is really a program of destruction. The program tricks the user into running it by proclaiming to perform some useful function, however, once initiated it can be as destructive as a virus. Trojan horses are less of a danger because they are easily destroyed, you simply delete the program, and they contain no means of copying themselves independently.

The worm operates much like a virus, but is capable of travel along a network on its own. Perhaps the best known worm was the one created by Robert Morris, the son of an NSA official. Morris created a worm to seek out sites on the Internet by traveling along its many connections and copying itself onto remote computers. Morris's worm was not created to damage any systems and was relatively harmless, but he made an error in

creating the program. This error caused the worm to begin propagating itself at exponential rates, slowing down Internet sites and causing communications to come to a standstill. The reaction among Internet users and system administrators was mass hysteria. The following are some highlights of the events as they unfolded over the course of twelve hours.

**5:00 p.m. - Morris launches his worm onto the Internet.**
**8:00 p.m. - System operators at a computer system across the nation begin noticing that something is slowing their computer system down.**
**2:38 a.m. - The virus has spread onto many systems including the Lawrence Livermore National Laboratory, NASA Ames Laboratory, Los Alamos National Laboratory, and the Department of Defense's Milnet network.**
**- A worried system operator releases the following message onto the Internet. "We are currently under attack by a computer virus."**
**5:00 a.m. - An estimated 6,200 computers have been infected in the course of 12 hours. System operators begin breaking network connections to protect their systems. Later calculations revealed that only around 2000 computers had been attacked.**

Days later, system operators were still cleaning and containing the Internet worm which had caused over one million dollars in damage.[21] More importantly the vulnerability of the networking system was exposed, and it took a major incident to bring this about. Morris was convicted for the damage initiated by his worm and sentenced to three year's probation, a $10,000 fine and four hundred hours of community service.[22] Though Morris's actions were indeed illegal, he did manage to bring into the spotlight the issue of computer security. If one college student could do so much damage by accident, what could a nation or terrorist group do on purpose?

## Creating a Computer Security Agency

The above anecdotes illustrate just a few of the many issues in computer crime that demonstrate a weakness in our national security. Computer crime is an issue that has been avoided for the most part by the government of the United States. What little action taken has been either wrongly focused or stagnated by political bureaucracies. What else would explain a 38 percent compliance with a national act that is supposed to improve our national

security? This issue must be put into perspective. Would the United States accept such limited compliance on other issues of national security? During times of war would the U.S. military establish a communications channel that was 38 percent secure? What if a report from the Department of Defense cited that our nuclear missiles would reach their targets 38 percent of the time? Would you invest your money in a bank that complied with only 38% of the minimum security standards suggested by the government? Under any other circumstances these numbers would be unacceptable, why are they accepted for computer security?

There are several key problems in the U.S. approach to computer crime. First, efforts for the most part are uncoordinated and ineffective, with too many law enforcement agencies claiming jurisdiction over computer crime issues. The Secret Service deals with computer crime cases that entail some aspect of fraud. The Federal Bureau of Investigation handles domestic aspects of computer crime like theft of services, the creation of virii, and illegal intrusion. The National Security Agency deals with national security issues like encryption and communications that originate from other countries.[23] While these agencies should continue with these objectives, consideration should be given to a new agency for the digital age.

This agency should focus on aspects of computer security in the military, business and private sectors. For simplicity, this proposed agency will be referred to as the Computer Security Agency (CSA). The prime objective of the CSA would be to oversee the operation of all sensitive computer systems and to insure that all known security bugs are fixed shortly after they are discovered. Secondary objectives would be to promote and establish security objectives for businesses and private citizens.

The CSA would collect data on security holes in several ways. First, it would monitor the publications of the digital underground. Hackers produce several electronic and paper publications that discuss issues concerning their movement, as well as ways to enter into secure systems. Many federal agencies are using these publications as sources of

information already, but it is not in a coordinated effort, and often holes discussed in these journals go unchanged for months, allowing more hackers to enter into the systems. Unfortunately the United States government has chosen to initiate an attack on these publications, instead of addressing the security holes they describe. For example, a few years ago, the editor of the popular digital publication entitled Phrack, had his computer system seized and was brought up on charges for publishing an edited version of an AT&T file. The U.S. later dropped the charges when evidence was discovered that the file which AT&T claimed was worth $70,00, was available to the public for $10.00.

Recently the United States Congress has conducted an attack on one of the hacker print journals, arguing that it should be banned as a threat to national security. The threat to national security comes not from the publication or the people who read it, but from the government that fails to correct security holes. First Amendment rights cannot be abandoned in an effort to improve national security. By focusing on this issue instead of others the United States only reinforces the fact that it has been incapable of, or unwilling to show direction and initiative towards digital issues. The world of cyberspace[24] is a new playing field, and those inherent ideals used to regulate activity in the physical world must be abandoned for new broader set of ideals that promise to expand, not hinder, our electronic capabilities, that do not tread on the rights of the citizens who chose to dwell in these electronic communities.

Another objective of the proposed CSA would be to establish a central site for the collection and distribution of information that addresses the security concerns of businesses and universities. For relatively little cost the CSA could connect a host computer to the Internet that would provide a forum for computer security issues. In accordance with this forum the CSA could work closely with those businesses that are interested in securing the integrity of their computer systems. The CSA should also turn to another group for assistance: the digital underground.

## Hackers as a National Resource

The digital underground should be viewed as an asset. They use illegal means to fulfill their curiosity about the workings of computer technology because the system has denied them other means of accessing the digital realm they love. Harvard Law professor Laurence H. Tribe even advocates that access to technology may be a required goal of democratic society. He states:

> **It's true that certain technologies may become socially indispensable -- so that equal or at least minimal access to basic computer power, for example, might be as significant a constitutional goal as equal or minimal access to the franchise, or to dispute resolution through the judicial system, or to elementary and secondary education. But all this means (or should mean) is that the Constitution's constraints on government must at times take the form of imposing "affirmative duties": to assure access rather than merely enforcing "negative prohibitions" against designated sorts of invasion or intrusion.[25]**

There is such a thing as the patriotic hacker who is loyal to the ideals of the nation. For example, when news of Stoll's German hacker selling U.S. secrets to the KGB hit the underground many hackers responded with hatred towards the guy who had associated their movement with national espionage and threats to national security. They were willing to use their abilities to combat this problem, and were even willing to target Soviet computers for the Central Intelligence Agency. An interesting story about hacker contributions to society is the story of Michael Synergy and his quest for presidential credit information. Synergy decided one day that it would be interesting to look at the credit history of then President Ronald Reagan. He easily found the information he was looking for and noticed that 63 other people had requested the same information that day. In his explorations he also noticed that a group of about 700 Americans all appeared to hold one credit card, even though they had no personal credit history. Synergy soon realized that he had stumbled upon the names and addresses of people in the U.S. government's Witness Protection Program. A good citizen, he informed the FBI of his discoveries and the breach of security in the Witness Protection Program.[26]

One of the basic benefits to United States national security is the lack of a coherent movement among the members of the digital underground. Hackers are by nature individualistic. They lack a common bond that allows them to focus their energies on one target. If there is a target of the hacker movement it is corporate America, especially the telephone companies. These corporations have arisen as a target because hackers rely on their service to access cyberspace, which can be a very expensive proposition for an unemployed teenager. The United States government has a vested interest in not providing them with another target, especially if that target is the government itself. The United States should accept the hackers and give them recognition for the service they provide in finding security holes in computer systems.

The United States should not discontinue efforts to stop credit fraud and other computer activities that are surely criminal. Instead the United States should allow the hackers to conditionally roam the realm of cyberspace. These conditions would include the following: (1) If computer access is gained, the security hole should be immediately reported to the CSA and should not be given to anyone else, and (2) information files should not be examined, modified or stolen from the site. In return the United States simply offers to give the hackers recognition for their accomplishments, feeding their competitive egos. Why should the United States government trust hackers? No trust is necessary, we are not offering the hackers anything that they don't already have, except recognition for their ability to discover security flaws. The hackers will remain on the networks regardless of what policy the United States follows concerning their activity, we are simply giving them the forum they need to meet people with similar interests on a legitimate basis, rather than a secret one. Robert Steele argues, "If someone gets into a system, that is not a violation of law, it is poor engineering. When we catch a hacker, rather than learn from him, we kick him in the teeth. When the Israelis catch a hacker, they give him a job working for the Mosad."[27]

Many U.S. corporations already trust the hackers to identify security weaknesses in their computer systems. The Legion of Doom, the most notorious group of hackers in the U.S., briefly entered the computer security business with the formation of their company called Comsec Security. Bruce Sterling reports, "The Legion boys are now digital guns for hire. If you're a well-heeled company, and you can cough up enough per diem and air-fare, the most notorious computer hackers in America will show up right on your doorstep and put your digital house in order - guaranteed."[28] Some argue that this is simply extortion, but individuals are not saying "pay up or else we will enter your system", they are offering to use their skills to protect you from other electronic intruders.

Hackers can be used as an asset to secure the United States' digital house, and every effort should be made not to alienate them from the newly emerging digital world. In the same Congressional hearing where his publication was branded as manual for computer crime, Emmanuel Goldstein made the following remarks about access to technology and computer crime:

> **This represents a fundamental change in our society's outlook. Technology as a way of life, not just another way to make money. After all, we encourage people to read books even if they can't pay for them because to our society literacy is a very important goal. I believe technological literacy is becoming increasingly important. But you cannot have literacy of any kind without having access.... If we continue to make access to technology difficult, bureaucratic, and illogical, then there will also be more computer crime. The reason being that if you treat someone like a criminal they will begin to act like one.[29]**

However, this represents only one threat to national security, the computer intruder. The CSA would also deal with problems such as virii, trojan horses and worms. Another function of the CSA would be to act as central site for information about new virii as well as providing, for free, programs to combat them. This would anger many software companies because it would hurt their business, but again protection from virii should not be made a purchasable commodity, at least not at the base level. Charging for a service that some people cannot afford ensures that some people will be unable to protect their system from computer virii which only helps spread their destruction to other computers.

The CSA would also be responsible for training government agencies on proper security techniques and ensuring that such preventions are being taken. The largest security hole in computer systems is the human factor. A whole book has been written devoted to this aspect of computer crime.[30] If you place a computer in a locked room with no outside connections you have a secure computer, give one person access and security is reduced. Give another person access and security is reduced even further. Now the two people can be used against each other with methods of social engineering. Consider the following true anecdote where a hacker named Susan demonstrates her social engineering skills:

> **As Susan later told the story, a team of military brass...from three services sat at a long conference table with a computer terminal, a modem, and a telephone. When Susan entered the room, they handed her a sealed envelope containing the name of computer system and told her to use any abilities or resources that she had to get into that system. Without missing a beat, she logged on to an easily accessible military computer directory to find out where the system was. Once she found the system in the directory, she could see what operating system it ran and the name of the officer in charge of that machine. Next, she called the base and put her knowledge of military terminology to work to find out who the commanding officer was at the SCIF, a secret compartmentalized information facility. Oh yes, Major Hastings. She was chatty, even kittenish. Casually, she told the person she was talking to that she couldn't think of Major Hasting's secretary's name. "Oh" came the reply. "You mean Specialist Buchanan." With that, she called the data center and switching from nonchalant to authoritative, said, "This is Specialist Buchanan calling on behalf of Major Hastings. He's been trying to access his account on the system and hasn't been able to get through and he'd like to know why"...Within twenty minutes she had what she later claimed was classified information up on the screen. Susan argued "I don't care how many millions of dollars you spend on hardware, if you don't have people trained properly I'm going to get in if I want to get in."[31]**

There are fundamental security measures that can be taught to system users to ensure that the security of the system is not compromised. The CSA would work toward ensuring that scenarios like the one illustrated above are not regular occurrences.

## The Schwartau Scenario

Are the nation's computers really in as much danger as this paper suggests? In 1991, writer Winn Schwartau released a fictional novel that addresses the threat to our national security that is inherent with our laxidasical computer security. Schwartau argues

that the reason he chose to tell the tale in the fictional format was "necessitated by a need to reach the largest possible audience."[32] That is because the fictional events in Schwartau's novel could easily become reality. Schwartau outlines a perfect attack on the infrastructure of the United States based on the weakness of our computer systems.[33] In Schwartau's novel the attacker is a Japanese businessman seeking revenge for the United States attack on Hiroshima. In reality this attack could be undertaken by any coalition with the proper resources. The United States could be brought to its knees by an attack on its computers and telecommunications systems.

## Computers and the International Community

Another difficult question that must be answered: what to do with nations that abide by different laws concerning computer crimes? The hackers that attacked the Department of Defense computers during the Gulf War were Dutch, because at the time hacking was legal there. How should the United States deal with such attacks? If the arguments made here were policy, there would be no need to address this issue. The Dutch hackers used known security holes to enter the computer systems, and one of the main objectives of the CSA is to ensure that such holes are fixed to prevent further attacks. It takes a lot more skill and ingenuity to break into a computer system if all known security holes have been effectively patched. You must actually hack the system to find new security holes which requires a great deal of time and the more time you spend on a secure computer system the more likely the chance of someone noticing your unauthorized presence. If an attack on the U.S. information infrastructure is initiated by another country's government it should be considered an act of war.

On the virus front there is little the United States can do to prevent the proliferation of virii in other countries. Attempts could be made to regulate all software coming from countries like Bulgaria into the United States, but that would be very difficult since files can be transferred over phone lines. This represents a severe threat to computer operations, but

the fact is that all aspects of computer crime cannot be controlled, just as the drug problem within the United States cannot be controlled. The best means available to combat these problems includes educating people about virus threats, and providing some forms of protection for free.

## Conclusion: The Challenge of the Digital Age

The digital age promises to change many aspects of our society. Mitchell Kapor writes:

> **Life in cyberspace is more egalitarian than elitist, more decentralized than hierarchical...it serves individuals and communities, not mass audiences. We might think of cyberspace as shaping up exactly like Thomas Jefferson would have wanted: founded on the primacy of individual liberty and commitment to pluralism, diversity, and community.[34]**

As a society we have much to learn about ourselves through this new medium of communication. A recently released book deals with aspects of electronic communities and the virtual world of cyberspace.[35] As a nation the United States must make sure that the structure it is building has a strong foundation and that weaknesses in that structure are not used to destroy it. It is a difficult task, because the constitutionally guaranteed rights of citizens cannot be infringed upon in the process. However, it is a task we must undertake. These are issues we must address. By not addressing these issues now the future of our country is being jeopardized. A handful of concerned citizens attempt to bring issues surrounding cyberspace to our attention everyday. Some of these issues concern national security, others concern individual privacy. Cyberspace has empowered the average person to explore and question the structure of our society and those that benefit from the way it is operated. Fundamental issues arise from hacker explorations. We must chose as a nation how to deal with these issues. Recent efforts in cloning produced a human fetus. The scientists that achieved this remarkable feat, immediately halted research arguing that a

public debate must arise to deal with the ethical and moral issues surrounding this technology. They argued that before experimentation in cloning continued, we must decide as a society which direction that the new technology will go, what ends we hope to achieve, and what the limits on its use should be. A similar debate on the issues of cyberspace must take place. There is no need to stop the technology, but we must decide which direction we want the technology to go, what rules will govern its use. We must do this now, before the technology starts dictating the rules to us, before it is too late to make changes in the basic structure of cyberspace without destroying the whole concept.

## Notes

[1]Wired Magazine (1993). Introduction. Volume One, Issue One.

[2]*Big Dummies Guide to the Internet* [Online]. Available FTP: ftp.eff.org Directory: pub File: bigdummy.txt

[3]Steele, Robert D. (1994). Hackers and Crackers: Using and Abusing the Networks. Presentation at the Fourth Annual Conference on Computers, Freedom and Privacy, Chicago, IL.

[4]For a more detailed introduction to the hacker movement read Steven Levy's Hackers: Heroes of the Computer Revolution. New York: Dell Publishing. 1984

[5]Sterling, Bruce (1992). The Hacker Crackdown: *Law and Disorder on the Electronic Frontier*. New York: Bantam Books. Pg 59

[6]Phrack, Volume One, Issue 7, Phile 3.

[7]Phrack Volume Four, Issue 40

[8]Stoll, Clifford (1989). The Cuckoo's Egg: *Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday.

[9]Hafner, Katie, & Markoff, John (1991). Cyberpunk: *Outlaws & Hackers on the Computer Frontier*. New York: Simon & Schuster. Pg 172

[10]Denning, Peter J. (1991). Computers Under Attack: *Intruders, Worms & Viruses*. New York: A.C.M. Press. Pg 183

[11]United States General Accounting Office. (1990). Report on Implementation of Computer Security Act. Washington, D.C. : U.S. Government Printing Office.

[12]United States General Accounting Office. (1990). Report on Implementation of Computer Security Act. Washington, D.C. : U.S. Government Printing Office.

[13]Sterling, pg 158

[14]Nathan, Paco Xander. (1993, May/June). *Jackson Wins, Feds Lose*. Wired Magazine, pg 20.

[15]Brock, Jack L. (1991). Testimony in Hackers Penetrate D.O.D. Computer Systems: Hearings before the Subcommittee on Government Information & Regulation, Committee on Governmental Affairs, United States Senate, November 20 , 1991.

[16]Brock testimony, pg 25

[17]Brock testimony, pg 29

[18]Mungo and Clough, pg 107

[19]Mungo, Paul, & Clough, Bryan (1992). Approaching Zero: *The Extra-ordinary Underworld of Hackers, Phreakers, Virus Writers & Keyboard Criminals*. New York: Random House.

[20]Mungo and Clough, pg 108

[21]Mungo and Clough, pg 98

[22]Hafner and Markoff, pg 345

[23]Most recently the NSA has been dealing with issues of encryption based around the RSA algorithm that provides better standards of encryption that the government approved Data Encryption Standard. Recently a movement has originated in the digital world to ensure encryption capabilities fall in the hands of private citizens to protect their right to privacy. The government has proposed a system were citizens must register the keys to their encryption system with the government so that they may be used where federal warrants call for monitoring of communications. This conflict promises to be one of the hot issues of the next year, and the future of electronic communications rests heavily on its outcome.

[24]The term cyberspace has varying definitions. It was original coined by William Gibson in his novel Neuromancer to define that place inside the computer where electronic communications/activities take place. Gibson describes it as "A conceptual hallucination experienced daily by billions of legitimate operators, in every nation...A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in nonspace of the mind, clusters and constellations of data. Like city lights, receding." Though we have yet to achieve this graphical representation of data that Gibson envisioned, data and its electronic place of residence are still referred to as cyberspace. More recently, John Barlow stated that "Cyberspace is where you are when you are talking on the telephone." For more information about the concepts and terms of the digital age, read Mondo 2000: A User's Guide to the New Edge, published by HarperPerennial.

[25]Tribe, Laurence H. (1991) The Constitution in Cyberspace Paper presented at the First Annual Conference on Computers, Freedom and Privacy Conference, Burlingame, CA.

[26]Mungo and Clough pg 57

[27]Steele, Robert D. (1994). Hackers and Crackers Using and Abusing the Networks. Presentation at the Fourth Annual Conference on Computers, Freedom and Privacy, Chicago, IL.

[28]Phrack Volume Three, Issue 33, Phile 10

[29]Goldstein, Emmanuel. (1993) Testimony before House Subcommittee on Telecommunications and Finance. Washington, D.C.

[30]Van Duyn, J. (1985). The Human Factor in Computer Crime. Princeton, NJ.: Petrocelli Books

[31]Hafner and Markoff, pg 60-61

[32]Schwartau, Winn (1991). Terminal Compromise. U.S.A.: Inter.Pact Press. Pg 0.

[33]Schwartau is currently working on a non-fictional computer security book entitled "Information Warfare: How to Wage and Win War in Cyberspace."

[34]Kapor, Mitchell. (1993, July/August) *Where is the Digital Highway Really Heading? The Case for a Jeffersonian Information Policy*. Wired Magazine , pg 53-59.

[35]The book is entitled Virtual Communities by Howard Rheingold. Though I have yet to read this book, I have read his book Virtual Reality, and it was very well written and informative.

# BIBLIOGRAPHY


Anonymous (1985 - 1994). Phrack Magazine. Volumes 1 - 42.

Bequai, August (1987). Technocrimes. Lexington, MA.: D.C. Heath & Company.

BloomBecker, Buck (1990). Spectacular Computer Crimes: *What They Are and How They Cost American Business Half a Billion Dollars a Year*. Homewood, IL.: Dow Jones-Irwin.

Brock, Jack L. (1991). Testimony in Hackers Penetrate D.O.D. Computer Systems: Hearings before the Subcommittee on Government Information & Regulation, Committee on Governmental Affairs, United States Senate, November 20 , 1991.

Denning, Peter J. (1991). Computers Under Attack: *Intruders, Worms & Viruses*. New York: A.C.M. Press.

French, Norman (1993). *Son of P.G.P.* Mondo 2000, No. 9 pp. 13 - 15.

Glickman, Dan (1991). Testimony in Regarding the Computer Security Act: Hearings before the Subcommittee on Government Information & Regulation, Committee on Governmental Affairs, United States Senate, November 20 , 1991.

Goldstein, Emmanuel. (1993) Testimony before House Subcommittee on Telecommunications and Finance. United States House of Representatives. June 9, 1993.

Hafner, Katie, & Markoff, John (1991). Cyberpunk: *Outlaws & Hackers on the Computer Frontier*. New York: Simon & Schuster.

Levy, Steven (1993, May/June). *Crypto Rebels*. Wired Magazine, pp. 54 - 61.

Levy, Steven (1984). Hackers: Heroes of the Computer Revolution. New York: Dell Publishing.

Mungo, Paul, & Clough, Bryan (1992). Approaching Zero: *The Extra-ordinary Underworld of Hackers, Phreakers, Virus Writers & Keyboard Criminals*. New York: Random House.

National Academy Press. (1991). Computers at Risk: *Safe Computing in the Information Age*. New York.

Parker, Donn B. (1976). Crime by Computer. New York: Charles Scribner's Sons.

Schultz, Eugene Jr. (1991). Testimony in Computer Security: Hearings before the Subcommittee on Government Information & Regulation, Committee on Governmental Affairs, United States Senate, November 20 , 1991.

Schwartau, Winn (1991). Terminal Compromise. U.S.A.: Inter.Pact Press.

Sterling, Bruce (1992). The Hacker Crackdown: *Law and Disorder on the Electronic Frontier*. New York: Bantam Books.

# BIBLIOGRAPHY

Stoll, Clifford (1989). The Cuckoo's Egg: *Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday.

Swartz, Peter (1993, July/August). *Post-Capitalist: Conversation with Peter Drucker*. Wired Magazine, pp. 80 - 84.

United States General Accounting Office. (1989). Report on Instances of Unauthorized Access to Space Physics Analysis Network(SPAN). Washinton, D.C.

United States General Accounting Office. (1990). Report on Implementation of Computer Security Act. Washinton, D.C.

Van Duyn, J. (1985). The Human Factor in Computer Crime. Princeton, NJ.: Petrocelli Books.

# THIRD INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, 1994 Volume I - Link Page


| | |
|---|---|
| Previous | OSS '94 Dr. Elizabeth D. Liddy, Information Retrieval via Natural Language Processing -or- An Intelligent Digital Librarian, |
| Next | OSS '94 Robert David Steele, Communications, Content, Coordination, and C4 Security: Talking Points for the Public Interest Summit, |

**Return to Electronic Index Page**