Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastruct

In today's electronic age, we rely on computers and the information they carry in almost every aspect of our lives. Whether it is banking, e-commerce businesses, health care, law enforcement, air transportation, college students, or your home Internet surfer, we are all becoming increasingly reliant upon the ones and zeros flying across the vast seas of interconnected wires, routers, switches, RF and cellular communication towers, and computer networks. It is these connected networks that now make up our national "cybe...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Shannon M. Lawson
SANS GSEC
Version 1.2F

Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure

Abstract:

In today's electronic age, we rely on computers and the information they carry in almost every aspect of our lives. Whether it is banking, e-commerce businesses, health care, law enforcement, air transportation, college students, or your home Internet surfer, we are all becoming increasingly reliant upon the ones and zeros flying across the vast seas of interconnected wires, routers, switches, RF and cellular communication towers, and computer networks. It is these connected networks that now make up our national "cyber" infrastructure. Yet it is this infrastructure that if not protected, may be prone to information warfare attacks by cyberterrorists.

The purpose of this paper is to explore the possibility of a terrorist group launching an information warfare attack against our infrastructure and to answer the question: Is the US ready to defend against a cyber attack?

I will define cyberterrorism, information warfare, from both an offensive and defensive standpoint, and define the aspects of the national infrastructure. I will examine the current trends of terrorist groups and focus on their information warfare capabilities to see if it is possible for a group like Hammas, Hezbolla, or al- Qaeda to commit to an all out information warfare attack aimed at crippling or destroying the US infrastructure. Finally, I will analyze the current US posture towards cyber warfare and terrorism. Are we ready to withstand an attack? Are we ready to not only withstand the attack but are we able to still function as a nation during and after the attack? I will present examples that suggest that the US is not prepared for this kind of warfare. I will offer suggestions as to what some organizations can do now to shore up their defenses and what the US government is doing in terms of national defense since the terrorist attacks on September 11, 2001.

Defining Cyberterrorism, IW, and the Aspects of the US Critical Infrastructure

Cyberterrorism, as defined by Dorothy E. Denning during her testimony before the Special Oversight Panel on Terrorism, is:

> "…the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objections. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at the least

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

> cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples."[1]

It is necessary to differentiate between a script kiddie hacking a system for fun and an organized group of extremists whose intent it is to cause massive economic and physical damage via the Internet to further their cause. It is important to make distinctions between the two because of the level of response that may be used to combat the attack.

Information Warfare (IW) has been around since the dawn of war. Information warfare has been and remains a critical element in deciding the outcome of military battles. According to Denning, "Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary."[2]

IW can be broken down into two distinct parts, offensive and defensive information warfare. Offensive IW is designed to prevent or alter information from being of any use to the defense in order to benefit the offense. The goal of defensive IW is to protect the information from attack. "Defensive information warfare is closely related to information security", according to Denning.[3]

Information warfare can be committed with almost anything that contains information that is deemed valuable to one side or the other. IW can span across many different facets of information media. It is way beyond the scope of this paper to discuss all forms of information warfare. However, this paper will focus on computer related IW in both an offensive and defensive nature as it pertains to both the United States' infrastructure and cyberterrorism.

The US national infrastructure is critical to day to day activities. Without it, airplanes could not fly, banks could not conduct financial transactions, emergency services would cease to function, and the government would lose its control. Therefore, without the national infrastructure, our national security would be in imminent danger. The following is a list of critical infrastructures each with a brief description that the United States deems to be of extreme importance as defined by Winn Schwartau in CyberShock:

1. Telecommunications: To include Internet, cable, cellular, telephone, satellite, and any other medium that connects systems together.
2. Electric Power
3. Oil and Gas Transportation: From the Alaska pipeline to oil refineries to natural gas distribution.
4. Transportation: Ground deliveries, air traffic control, and trains. All of which play a huge role in delivering food and materials, driving businesses and tourism.

---

[1] Denning, Congressional Testimony.
[2] Denning, Information Warfare and Security, p.10.
[3] Denning, Information Warfare and Security, p.12.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

5. Banking and Finance: The movement of trillions of dollars of virtual money through brokerages and banks over computer wires and networks.
6. Water Supply: Managing the water supply and waste disposal is done by electronic means.
7. Emergency Services: 911, fire and police departments, rescue units all rely upon the communications networks to do their job with speed and efficiency.
8. Continuity of Government: During an attack, can the government survive and maintain control of a city, state, or the country?[4]

These infrastructures are of the utmost importance to protect. Without them, our country would be brought to its knees. They are, therefore, prime targets for terrorists. Our physical infrastructure may be protected but what about the cyber-infrastructure? This is the collection of infrastructures that are now connected to each other through the Internet. Was the cyber-infrastructure designed with security in mind? According to Congressman Ciro Rodriguez,

> "And though the benefits of the Internet are clear, the widespread network of interconnected computer systems also poses significant risks to our national security. The same cyber technology that connects our homes, our schools and our businesses to the rest of the world, if not properly protected, may also provide terrorists with the tools they need to launch cyber attacks against our nation."[5]

The threat may not come from a terrorist with a gun or a bomb. It may come from a terrorist armed with nothing more than a keyboard, a mouse, and a connection to the Internet.

Cyberterrorism

This section of the paper will focus on who are the cyberterrorists and examine some of the technologies that they are using to conduct information operations. Additionally, it will look at the feasibility of terrorist groups conducting information warfare from both a geographic and a technological standpoint.

Who are the cyberterrorists? Many of the more traditional terrorist groups such as Hezbolla, Islamic Jihad, Hammas, and al- Qaeda have discovered the use of the Internet as a way to promote their cause and conduct their terrorist operations. Several months ago, you could log onto attrition.org's website and view the web defacement mirror pages. Many of the mirrored pages were of Arab terrorist and hacktivist groups hacking Israeli sites and vice versa. Though web defacement is common among hacker groups, it is a clear indication that the radical terrorist groups are realizing the power of the Internet and information warfare. Here they could "attack" their enemy without losing one of their own through suicide attacks. They are able to spread their message and even post graphic pictures on prominent websites at will. Some important factors regarding cyberterrorists are motivation and capability. Groups such as Hammas and Hezbolla are able to commit simple web defacements, but that does not mean they are capable of taking down key US infrastructures. These groups do have the motivation and in some cases, such as al-Qaeda, have the financing to hire the hackers to attack via the Internet. However, do the hackers

[4] Schwartau, p.396-397.
[5] Rodriguez, p.1.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

have the motivation to inflict massive amounts of damage and even death? One hacking group that arose from the recent conflict between Israel and Palestine is the Iron Guard. It is reported that they have ties to Hezbolla and other Islamic extremist groups. Iron Guard's call for cyber Jihad was supported by al- Muhajiroun who has known ties to Osama bin Laden.[6]

Other groups that have been in the press recently include al- Qaida Muslim Alliance crew, Muslim Online Syndicate, GForce Pakistan, and PHC (Pakistan Hackers Crew). Would it be possible for figureheads like bin Laden to recruit hacker groups, whom already have a hatred for the US and Israel, to plan and execute a full-scale cyber attack on the US? What about the capability of the terrorist organizations to commit a cyber attack? According to the Office of Critical Infrastructure Protection and Emergency Preparedness' threat analysis of the al- Qaeda cyber capability, it is highly unlikely due to the telecommunications limitations in Afghanistan for bin Laden or any member of the organization to attack the US via the Internet. However, it is known that groups like bin Laden's activates sleeper cells to commit acts of terrorism and it is proven that they have cells operating all over the world. Could they use those cells in a coordinated cyber attack?[7]

Recently, terrorist groups have been conducting more passive forms of information warfare. It is reported that these terrorist groups are using the Internet to conduct their operations by employing email and file encryption and steganography, as well as conducting web defacement attacks. According to an article by Will Knight, the al- Qaeda organization was using encryption, 40 bit Data Encryption Standard (DES), to cloak its files in two computers that were recovered by Northern Alliance forces in Afghanistan. Though the encryption used was relatively weak, the use of encryption shows that these groups are now using more hi-tech methods to mask their operations.[8] Other groups that have used encryption to mask their terror operations, according to an essay by Dorothy Denning and William E. Baugh Jr. include the Aum Shinri Kyo who launched the nerve gas attack in the Tokyo subway in 1995. The Aum Shinri Kyo encrypted their computer files relating to their plan of deploying weapons of mass destruction in Japan and the United States. Ramsey Yousef, who was apart of the terrorist plot to blowup the World Trade Center in 1993 and a Manila Air airliner, had encrypted his plans of future terrorist operations that included the bombing of eleven airliners.[9]

Another tool in the cyberterrorist toolbox is steganography. Denning and Baugh define steganography as the "methods of hiding secret data in other data such that its existence is even concealed. One class of methods encodes the secret data in low-order bit positions of image, sound, or video files."[10] When email is encrypted and sent over the wire, it appears differently through an analyzer than does typical Internet traffic. Therefore, who ever may be sniffing for traffic may be interested to know what is so important that it needs to be encrypted. However, steganography works differently by allowing the user to insert a text document, picture, audio or video clip into another document. For example, a terrorist could insert a picture of their next target into the "." of a normal text document such as a letter. He could then email that letter with

[6] OCIPEP, p.3.
[7] OCIPEP, p.2-3.
[8] Knight, p.1.
[9] Denning and Baugh Jr., p.167.
[10] Denning and Baugh Jr., p.175

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the hidden document in the”.”. Anyone sniffing the traffic probably would not give it a second thought because it blends in to typical Internet traffic. In some steganography suites, it is possible to encrypt your file, whether it is audio, video, or picture, before you insert it into your document. This tool is even available for free on the Internet.

How feasible is it that a group such as al-Qaeda could launch an information warfare attack against the United States? One factor is geography. According to the Canadian OCIPEP, the telecommunications infrastructure of Afghanistan could not support such an attack. OCIPEP states, “According to the CIA World Fact Book, the capital city of Kabul had only 21,000 main phone lines in use in 1998. Domestically, there are telecommunication links between the cities of Mazar –e Sharif, Heart, Kandahar, Jalalabad, and Kabul through microwave and satellite systems. Osama bin Laden’s personnel reportedly go to Peshawar, Pakistan to maintain phone, fax, and modem communication with the outside world.”[11] It is more likely that bin Laden’s forces will have to travel outside Afghanistan to conduct an information warfare attack. Pre-arranged terror cells from around the world could be activated to conduct the coordinated attack. Many of these terrorist groups posses both the charisma and finances to hire hacker sympathizers to conduct information warfare operations. Dorothy Denning in her testimony before the Special Oversight Panel on Terrorism quoted Clark Staten, executive director of the Emergency Response and Research Institute in Chicago, that “members of some Islamic extremist organizations have been attempting to develop a ‘Hacker Network’ to support their computer activities and even engage in offensive information warfare attacks in the future.”[12] Another factor is the complexity of an information warfare attack weighed against that of a physical attack. It is obviously more technically difficult to wage an information attack than to strap explosives to yourself. Traditional terrorists may use cyberspace to communicate with other operatives around the globe but may stick to the known terrorist methodology of using car bombs, hijackings, and kidnapping.

Security Posture of the US Critical Infrastructure

This section of the paper will attempt to examine the current security posture of the United States and its critical infrastructure by answering the following questions. Are they vulnerable to terrorist cyber attacks? Could a hacker-for-hire group gain access to our most critical systems and hold us hostage? What can companies and even US citizens do to protect our systems from attack? Has our views changed since the terrorist attacks on September 11, 2001?

Is the US ready to defend itself against a cyber attack of immense proportions? This is a difficult question to answer due to several reasons. First, the United States has not been tested under a real information warfare attack. Some companies have lost millions due to denial of service attacks. The Department of Defense has had its systems probed and penetrated several times. However, the country has never been a victim of a full-scale cyber attack. Second, the United State’s cyber defense and offense capabilities are a well-guarded secret for obvious national security reasons. There are some reports that hint at the current readiness though. In 1997, the National Security Agency (NSA) ran an operation called Eligible Receiver. The

[11] OCIPEP, p.3.
[12] Denning, Congressional Testimony, p.2.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

following article by Bill Gertz describes how teams of hackers from NSA were able to disable major components of the US infrastructure and for the most part, went undetected from the FBI.

> "Computer hackers could disable military; System compromised in secret exercise
> Senior Pentagon leaders were stunned by a military exercise showing how easy it is for hackers to cripple US military and civilian computer networks, according to new details of the secret exercise.
> Using software obtained easily from hacker sites on the Internet, a group of National Security Agency officials could have shut down the US electric-power grid within days and rendered impotent the command-and-control elements of the US Pacific Command, said officials familiar with the war game, known as Eligible Receiver.
> "The attack was actually run in a two-week period and the results were frightening," said a defense official involved in the game. "This attack, run by a set of people using standard Internet techniques, would have basically shut down the command-and-control capability in the Pacific theater for some considerable period of time."
> Pentagon spokesman Kenneth Bacon said, "Eligible Receiver was an important and revealing exercise that taught us that we must be better organized to deal with potential attacks against our computer systems and information infrastructure."
> The secret exercise began last June after months of preparation by the NSA computer specialists who, without warning, targeted computers used by US military forces in the Pacific and in the United States.
> The game was simple: Conduct information warfare attacks, or "infowar," on the Pacific Command and ultimately force the United States to soften its policies toward the crumbling communist regime in Pyongyang. The "hackers" posed as paid surrogates for North Korea.
> The NSA "Red Team" of make-believe hackers showed how easy it is for foreign nations to wreak electronic havoc using computers, modems and software technology widely available on the darker regions of the Internet: network-scanning software, intrusion tools and password-breaking "log-in scripts."
> According to US officials who took part in the exercise, within days the team of 50 to 75 NSA officials had inflicted crippling damage.
> They broke into computer networks and gained access to the systems that control the electrical power grid for the entire country. If they had wanted to, the hackers could have disabled the grid, leaving the United States in the dark.
> Groups of NSA hackers based in Hawaii and other parts of the United States floated effortlessly through global cyberspace, breaking into unclassified military computer networks in Hawaii, the headquarters of the US Pacific Command, as well as in Washington, Chicago, St. Louis and parts of Colorado.
> "The attacks were not actually run against the infrastructure components because we don't want to do things like shut down the power grid," said a defense official involved in the exercise. "But the referees were shown the attacks and shown the structure of the power-grid control, and they agreed, yeah, this attack would have shut down the power grid."
> Knocking out the electrical power throughout the United States was just a sideline for the NSA cyberwarriors. Their main target was the US Pacific Command, which is in charge of the 100,000 troops that would be called on to deal with wars in Korea or China.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

> "The most telling thing for the Department of Defense, when all was said and done, is that basically for a two-week period the command-and-control capability in the Pacific theater would have been denied by the 'infowar' attacks, and that was the period of the exercise," the official said.
> The attackers also foiled virtually all efforts to trace them. FBI agents joined the Pentagon in trying to find the hackers, but for the most part they failed. Only one of the several NSA groups, a unit based in the United States, was uncovered. The rest operated without being located or identified.
> The attackers breached the Pentagon's unclassified global computer network using Internet service providers and dial-in connections that allowed them to hop around the world.
> "It's a very, very difficult security environment when you go through different hosts and different countries and then pop up on the doorstep of Keesler Air Force Base [in Mississippi], and then go from there into Cincpac," the official said, using the acronym for the Commander in Chief, Pacific.
> The targets of the network attacks also made it easy. "They just were not security-aware," said the official.
> A second official found that many military computers used the word "password" for their confidential access word."[13]

This was just an exercise to prove what real-world cyberterrorists or rogue nation states could do. That was five years ago. On November 9, 2001 several reports were issued about US government agencies failing in a computer security review. The congressional Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations began investigating major executive branch departments after Congress passed the Government Information Security Reform Act. This act requires that Federal Agencies establish and maintain a computer security program. According to Scartlett Pruitt of the IDG News Service, "Critical agencies such as the Department of Defense, Department of Transportation, Department of Health and Human Services, and Department of Energy, as well as the Nuclear Regulatory Commission, all received "F's", a failing grade."[14] Pruitt also quoted Subcommittee Chairman Rep. Stephen Horn (R-Calif.), "Without proper protection, the vast amount of sensitive information stored on government computers could be compromised and the systems themselves subject to malicious attacks… As the recent spate of computer viruses and worms have shown, cyber attacks have the potential to cause great damage to the nation."[15] These departments represent the head of each of the critical infrastructures. If the NSA hackers were able to take down parts of the infrastructure and several years later some of the top agencies are receiving failing grades in computer security, how long will it take for terrorists to exploit those major vulnerabilities in the infrastructures?

The US government is not the only one that can be a target for terrorists. US companies also play a role in protecting the national infrastructure. After the events of 9/11, the airline industry came to a halt. Tourism was affected as was long distance deliveries of goods and even the mail. Banks may be inclined to shut down their systems during and after a cyber attack

[13] Gertz, p.1-2.
[14] Pruitt, p.1.
[15] Pruitt, p.2.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

therefore causing a denial of service to its customers. The possibilities are endless. What can these companies do to help shore up defenses?

Private industry and the government can start using email and file encryption to conceal their operations and prevent sensitive data from unauthorized disclosure, whether national security secrets or private customer account data or confidential proprietary information. There are plenty of email and file encryption software programs available that are extremely easy to use.

A background check of new employees is an excellent security measure. This is a good defensive action from an information warfare standpoint. This can give employers a heads up on whom they are hiring before the new employee has physical access to a facility and sensitive documents. Background checks can be costly but even workers at the bottom of the hierarchy will have access to information or just the facility to conduct possible information warfare attacks.

In addition to the background checks is physical security. Depending on the business, it may be necessary to install badge swipes with access pin numbers or even hire security guards. Electronic keypads on server rooms that are not shut off in the event of power loss may be necessary for some companies. These are just a few examples physical security measures to secure a facility.

Firewalls, intrusion detect systems, access control lists, and anti-virus software are all components that companies may need. Some companies may find that they need one or the entire list above. Implement them with a strong security policy. The policy will tell the who, what, where, when, and how of your computer security operations. Make sure that the policy is updated regularly, signed off by management, and everyone in the IT department are familiar with it.

User training is a huge step in the right direction. Start training employees to lock their screens when they leave their desk. Use strong password management schemes. With Windows NT and 2000, there is no excuse for not using the built in strong password mechanisms. Teach employees about social engineering so that they are not duped into divulging potentially damaging information. When employees feel that they are taking an active role in protecting the company or agency they work for, they tend take more pride in what they do. The more they understand the policies set forth, the less potential problems there may be in future.

The bottom line is that as a potential target, you must cover all possible aspects of vulnerabilities in the firm. Defensive information warfare is a tough job. Michael Erbschloe states, “A fundamental dynamic of information warfare is that defenders must always succeed in protecting systems, whereas if attackers do not succeed, they can try again later or move onto another target that my be easier to steal information from, damage, or disable.”[16]

Nationally, there are several organizations that have stood up to help defend that national infrastructure. The FBI’s National Infrastructure Protection Center’s mission is to “serve as the

[16] Erbschloe, p.174.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

US government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures."[17] They are a link between government and the private industry. The President's Commission on Critical Infrastructure Protection was created on July 15, 1996. According to Shwartau, President Clinton signed an executive order, that created the PCCIP, which stated: "Certain national infrastructures are so vital that their incapacity or destruction would have debilitating impact on the defense of economic security of the United States."[18]

Since the deadly terrorist attacks on 9/11, not only the US but also the world has shifted gears towards defending against terrorism especially in the realm of cyber space. There have been dozens of articles written about the fears of a cyber assault committed by terrorists such as the article entitled "Doomsday Fears of Terror Cyber-Attacks" by the BBC News.[19] Some hackers have even taken matters into their own hands by attacking Islamic websites and ISPs abroad according to McWilliams of Newsbytes.[20]

There is now a global effort to fight information warfare. On November 23, 2001, thirty nations signed a global cybercrime treaty. "The convention streamlines definitions and civil penalties for hacking, copyright infringement, computer-related fraud, and child pornography. The treaty also includes provisions added in the wake of the September 11 terrorist attacks that give member states common powers to search and intercept the Internet communications of suspected terrorists."[21] This treaty is extremely important because prior to this there was no international cooperation for battling cybercrime. It was difficult to prosecute criminals/terrorists from other friendly nations let alone countries with which we have strained relations.

The US signed into law the USA Patriot Act which has expanded powers of government to read emails, intercept wireless communications, and monitor computer use to name a few. According to the article "Anti-terror Law Expands Powers", the act "requires information sharing among criminal investigators and intelligence officers."[22] Hackers may even face life imprisonment under the Anti-Terrorism Act. The list of terrorism offenses include "the provisions of the Computer Fraud and Abuse Act that make it illegal to crack a computer for the purpose of obtaining anything of value, or to deliberately cause damage. Likewise, launching a malicious program that harms a system, like a virus, or making an extortionate threat to damage a computer are include in the definition of terrorism" according to Kevin Poulsen.[23]

The Federal Bureau of Investigation will now allow police chiefs from cities, counties, and other municipalities to apply for a national security clearance. This would now keep the local law enforcement authorities abreast of all-terrorist watch lists and warnings. This is a huge step for the government because the communication between states and federal law enforcement was

[17] NIPC Website
[18] Schwartau, p.395.
[19] Hermida, p.1-3
[20] McWilliams, p.1-2.
[21] Krebs, p.1
[22] Matthews, p.1-2.
[23] Poulsen, p.1.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

virtually nonexistent. The idea is that by sharing information about terrorists and their activities will help the government prevent future incidents including cyberterrorism.[24]

In the wake of bin Laden's attack on America, it has been reported that both hackers and the US government may resort to cybertactics to freeze bin Laden's accounts and assets. According to Dan Verton, "hacking experts said it is well within the technical capabilities of the US intelligence community to make it disappear forever." Obviously there are many legal issues surrounding operations like this. However, it is a clear example of the US engaging in offensive information warfare.[25]

Conclusions

It is my opinion that the US infrastructures are extremely vulnerable. I equate it to poor airport security prior to 9/11. It took a tragedy of immense proportions for changes to be made. These changes were not hard. They were basic physical security measures that should have been taken and implemented a long time ago. Several planes crashed into the World Trade Center and the Pentagon. All air travel ceased for a week. The stock market closed also for a week and lost millions. Airports shut down and thousands of people were out of work. Airlines lost billions of dollars and were forced to lay people off and reduce flights. People were scared to fly because it was perceived that the security guards in the airports were not doing their jobs correctly and therefore, may allow more terrorists to slip through. It has already been proven that our infrastructures are vulnerable from Operation Eligible Receiver 1997. Will it take an attack of immense proportions for changes to be made? Dorothy Denning stated that "cyberterrorism is more of a theory."[26] Terrorists are using cyber technology to communicate but not as a weapon. What about the children of these terrorist groups? Technical books are plentiful, as are hands on courses. Who is to say that the computer savvy next generation of terrorists will not use the keyboard as their weapon? What kind of fear could they instill in people by being able to strike from almost anywhere on the globe? September 11th gave us a tangible enemy. Osama bin Laden and his al- Qaeda network. What enemy would we have with a cyber attack? You would have to find them first before you could stop them. Luckily, defensive information warfare gives us a goal. We can shore up our defenses. Even the average citizen can protect their "always on" PC and make it harder for the hackers and terrorists to use them as zombies in a distributed denial of service attack. Employees can be mindful of things they talk about after work or apply some common sense as they are throwing a customers' account statement into the trash with their name, account numbers and SSNs. Companies should be vigilant about the protection of their assets including the 1s and 0s. There will always be vulnerabilities. If we all play our part and work as a team to protect our infrastructure, the US critical infrastructure will be a formidable opponent.

[24] Miller, p.1.
[25] Verton, p.1-3.
[26] Denning, Congressional Testimony, p.2.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

Browning, Graeme. "Filling the Ranks- Agencies Scramble for Infosec Experts." 03 Dec 2001. URL: http://www.fcw.com/fcw/articles/2001/1203/mgt-ranks-12-03-01.asp (24 Jan 02).

Denning, Dorothy E. "Cyberterrorism." Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives. 23 May 2000. URL: http://www.terrorism.com/documents/denning-testimony.shtml (25 Jan 01).

Denning, Dorothy E. Information Warfare and Security. Reading: ACM Press, 1999. p. xiii-12.

Denning, Dorothy E. and Baugh, William E. Jr. "Encryption in Crime and Terrorism." Cyberwar 2.0.Fairfax: AFCEA International Press, 1998. p.167, 175

Erbschloe, Michael. Information Warfare- How to Survive Cyber Attacks. New York: McGraw-Hill Companies, 2001. p. 174

Garretson, Cara. "Panel: Government Info Sharing is Key to Fighting Terrorism." 19 Dec 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO66770,00.html (24 Jan 02).

Gertz, Bill. "NSA's Operation Eligible Receiver." 16 Apr 1998. URL: http://www.landfield.com/isn/mail-archive/1998/Apr/0091.html (24 Jan 02).

Hermida, Alfred. "Doomsday Fears of Terror Cyber-Attacks." 11 Oct 2001. URL: http://news.bbc.co.uk/hi/english/sci/tech/newsid_1593000/1593018.stm (24 Jan 02).

Johnson, Maryann and Radcliff, Deborah. "Cybersecurity Czar Urges More Spending to Protect IT Infrastructure." 08 Nov 2001. URL: http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_STO65468-,00.html (24 Jan 02).

Knight, Will. "Weakened Encryption Lays al- Qaeda Files." 17 Jan 2002. URL: http://www.newscientist.com/news/print.jsp?id=ns99991804 (24 Jan 02).
Krebs, Brian. "Thirty Nations Sign Global Cybercrime Treaty." 26 Nov 2001. URL: http://www.newsbytes.com/news/01/172398.html (24 Jan 02).

Matthews, William. "Anti-terror Law Expands Powers." 26 Oct 2001. URL: http://www.fcw.com/fcw/articles/2001/1022/web-terror-10-26-01.asp (24 Jan 02).

McWilliams, Brian. "Hackers Discuss Retaliatory Cyberstrikes." 12 Sep 01. URL: http://www.newsbytes.com/news/01/170025.html (24 Jan 02).

Miller, Jason. "FBI Puts Police Chiefs in the Security Loop." 20 Dec 01. URL: http://www.gcn.com/vol1_no1/daily-updates/17654-1.html (24 Jan 02).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

NIPC. URL: http://www.nipc.gov/about/about.htm (17 Feb 02).

Office of Critical Infrastructure Protection and Emergency Preparedness. "Threat Analysis- Al-Qaida Cyber Capability." 02 Nov 2001. URL: http://www.epc-pcc.gc.ca/emergencies/other/TA01-001_E.html (24 Jan 02).

Poulsen, Kevin. "Hackers Face Life Imprisonment Under 'Anti-Terrorism' Act." 24 Sep 2001. URL: http://www.securityfocus.com/news/257 (24 Jan 02).

Pruitt, Scarlett. "16 Agencies Flunk Computer Security Review." 09 Nov 2001. URL: http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_STO65589-,00.html (24 Jan 02).

Rodriguez, Ciro D. "Cyberterrorism- An Emerging Threat to National Security." 02 Dec 2001. URL: http://www.house.gov/rodriguez/ (24 Jan 02).

Salkever, Alex. "Toward More Cybersecurity in 2002." 02 Jan 2002. URL: http://www.securityfocus.com/news/302 (24 Jan 02).

Schwartau, Winn. CyberShock. New York: Thunder's Mouth Press, 2000. p. 395-397.

Stafford, Ned. "Sudan Bank Hacked, Bin Laden Info Found- Hacker." 27 Sep 2001. URL: http://www.newsbytes.com/news/01/170588.html (24 Jan 02).

Verton, Dan. "US Recovery: US Could Use Cybertactics to Seize bin Laden's Assets." 21 Sep 2001. URL: http://www.infoworld.com/articles/hn/xml/01/09/21/010921hnbinhack.xml?09

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced