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.

Issues in Protecting Our Critical Infrastructure

An increasing dependence on computers within our society brings with it an increasing vulnerability to disruption due to both physical and cyber-based attacks. An interruption of one or more of our infrastructure components can have far-reaching affects, having economic and even national security implications. Because of the dangers an interruption of critical infrastructure represents, our government has embarked on a mission to protect it. There are many stumbling blocks along the way, including legal and technical i...

Copyright SANS Institute
Author Retains Full Rights

AD

GSEC Practical Assignment v1.4b

Issues in Protecting Our Critical Infrastructure

William R. Nance

April 20, 2003

Abstract

The Internet has brought many important changes to the way we do business, both in the public and private sectors. We can use it to instantly communicate with others across the country, conduct business meetings, or control equipment in remote locations. These time and money saving benefits have been quickly incorporated into government and commercial operations across the United States. Transportation, communications, and power distribution systems are just some of the many services that have come to rely on computers and the Internet for their operations, and our society depends heavily on these services. This increasing dependence on computers within our society brings with it an increasing vulnerability to disruption due to both physical and cyber-based attacks. An interruption of one or more of our infrastructure components can have far-reaching affects, having economic and even national security implications.

Because of the dangers an interruption of critical infrastructure represents, our government has embarked on a mission to protect it. There are many stumbling blocks along the way, including legal and technical issues on both the domestic and international levels. The technological advances over the last several years have outpaced the ability of lawmakers to keep our laws up to date. The coordination of the many governmental agencies and private institutions involved, and the implementation of the procedures meant to protect our infrastructure are huge undertakings that continue to have problems. Law enforcement agencies face many challenges in being able to effectively investigate cyber attacks. All these challenges must be overcome, and protection of our infrastructure accomplished without violating the rights of individual privacy.

Critical Infrastructure

Critical infrastructure is composed of the basic services that we have come to depend on, and are necessary to support our society and ensure national stability. It includes transportation, communications, power distribution systems, banking and financial institutions, and basic government operations, including law enforcement, fire services and the military. Loss of, or damage to, one of these services can have significant consequences, such as an event that shuts down our communications systems. Communications is a valuable part of all infrastructure components, and loss of this one piece can hamper the operation of the rest. It can have grave consequences if emergency services cannot be reached in a life-threatening situation. In a daily-life situation, we might not be able to make a phone call to order pizza because the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

telephone service is out, while at the same time we're missing the latest episode of CSI because the television transmission facilities are down.

One real-life example of the interruption of one of the infrastructure components was seen in the aftermath of the September 11, 2001 attacks on the World Trade Center in New York City. This attack, using our own airlines as a weapon, caused the FAA to ground all commercial and private aircraft across the entire country. Initially, thousands of people were stranded. Some were able to rent cars to drive themselves home, but it wasn't long before there were no more rentals available. Not everyone was affected to this degree, but there were effects that touched everyone. Companies such as FedEx and UPS could not ship goods by air, and deliveries were slowed considerably. We couldn't watch the latest car chase live on our local news broadcasts, or hear up to the minute traffic conditions on the radio because their helicopters were not allowed in the air.

Another extreme example of the interruption of multiple components of a nation's critical infrastructure can be seen in the current war against Iraq. The first targets of our attack were those that supported the Iraqi government. Government installations, electric power generation, water pumping stations, and communications facilities were partially, if not completely, disabled. Transportation systems were interrupted when our soldiers began taking control of roads and towns, effectively shutting off the flow of goods and services. Even facilities that were not damaged by bombs and artillery shells were unmanned because the workers had fled the hostilities. An almost immediate effect on the Iraqi people was a lack of drinking water. With no government control, law enforcement and fire services were non-existent. Looting was rampant, even to the point that equipment was taken from hospitals, which were overflowing with patients, but were without medical staff to care for them. Fires burned until all available fuel sources were consumed.

What does this have to do with computer security? After all, doesn't computer security mean keeping hackers out of my system? Computer security does include protecting our systems from unauthorized access, but it also encompasses much more, including how to minimize both the amount of damage from an attack and the length of time a system and its data are unavailable after an attack. The previous examples illustrate physical attacks that hamper, if not completely destroy the means by which government, business and service providers operate. Damage to even one of the components of our infrastructure can greatly affect a nation's society, especially one such as ours that is so highly dependent upon computers for its daily operations.

The physical destruction of computer equipment can be viewed as an extreme example of a Denial of Service (DoS) attack — you've been denied service from that machine forever. Cyber attacks may be subtler than a physical attack, but may also be more effective than physical destruction, depending on the goals of the attacker.

Is the Threat Real?

In recent years, there have been many examples of computer systems being attacked and compromised. Independent hackers and script kiddies have been involved in many of these, but there are an increasing number of attacks that appear to be politically

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

motivated. During times of political tensions between countries and/or political organizations, an increase in cyber attacks is also seen. These attacks are typically web defacements, Distributed Denial of Service (DDoS) attacks, worms and Trojan horses, but there have also been root access penetrations. The levels of organization and sophistication of these attacks have been increasing (Cyber Attacks, Cyber Protests).

An example of a politically motivated cyber war is illustrated in the conflict between India and Pakistan over the Kashmir territory. There have been many cyber attacks against both sides of this conflict. Pakistani hackers have defaced many Indian web sites, including the Indian Parliament, the Indian Institute of Science, and the Bhabha Atomic Research center, from which they reportedly were able to retrieve nuclear research information (Cyber Attacks 5).

The Israeli/Palestinian conflict shows that cyber attacks can be tied to real-world incidents. The number of cyber attacks increase coincident with or immediately following political events such as car bombings, Israeli attacks on facilities suspected of being tied to terrorist organizations, or even after a breakdown of talks between Israel and the Palestinian Authority (Cyber Attacks 7).

The United States has had its own problems in this area. After the incident in which an American reconnaissance aircraft collided with a Chinese fighter, cyber attacks against both sides increased. The source of these attacks wasn't limited to the two countries directly involved, but both sides seemed to have plenty of support from around the world. It doesn't seem to matter whether or not the United States is directly involved in the conflict; we seem to be seen as a valid target of attacks. Pakistani and Palestinian sympathizers have also targeted web sites within the United States (Cyber Attacks 5,8; Cyber Protests 8).

Experts have grouped these attackers into four groups: terrorist organizations, targeted nation-states, terrorist sympathizers and anti-U.S. hackers, and thrill seekers. Terrorist organizations such as Al Qaeda have typically not been involved in actual cyber attacks, but have used the Internet for organizing, planning and spreading propaganda. Targeted nation-states are those that we suspect of harboring or promoting terrorism, and are viewed as possible U.S. targets in the war on terrorism. Many of these nation-states are suspected of having programs to develop the capability to engage in espionage and information warfare against the United States. This use of cyber attacks by one country against a much stronger country, such as the U.S., in times of military conflict is known as "asymmetric warfare," or the use of unconventional tactics against a foe of far greater military power. It is considered more likely that attacks will be seen from terrorist sympathizers and those with strong anti-U.S. views. Many of these groups are very well organized, and the possibility of two or more of these groups combining forces in a coordinated attack against the United States is very real. The thrill seekers are generally not well organized, and typically the attacks from those in this group are more nuisances than they are damaging or sustained. But attacks from those in this group can cause a considerable disruption of service (Cyber Attacks 12-14).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

During the war on terrorism, we should expect that these attacks will become more frequent, more sophisticated, more organized, and more damaging. Information warfare seems to be viewed by many countries as another weapon in their arsenals. We must be ready to protect the networks composing our infrastructure from these threats.

Legislative Changes

Protecting our critical infrastructure, from either physical or cyber-based attacks, spans both the public and private sectors, and will take a combined effort to ensure its security. It must be well coordinated, and requires close cooperation between all entities involved. The necessary laws must be in place to allow effective prosecution of cybercrime, both on the domestic and international levels.

Over the last several years, technology has advanced faster than the ability of legislation to keep up with it. Legislation that was enacted to cover telecommunications back when it was just the plain old telephone system (POTS) doesn't work considering the complexities of Internet traffic. For example, the laws distinguish between voice and non-voice communications and how they are to be treated in criminal investigations, but legislators didn't foresee the combining of both into a single e-mail, as became possible with the advent of Multipurpose Internet Mail Extensions (MIME) (Field sec. 209). Legislators have been playing a catch-up game to update the laws to keep up with technology. They must also balance the needs of law enforcement against the rights of individuals.

In recent years, there have been many changes from both the legislative and executive branches of government that address the need for protection of our critical infrastructure, define new and extend current laws to keep up to date with technological advances, and create new or reorganize existing departments. Some examples of legislation relating to Internet communications and infrastructure protection follow.

Computer Fraud and Abuse Act of 1986

The Computer Fraud and Abuse Act of 1986 (CFAA) laid out several offenses which are considered unauthorized access of computer systems, and the punishments for these offenses. It dealt mainly with those systems owned, operated, or used by government agencies, financial institutions, and medical services. The CFAA is one of the primary statutes used to prosecute computer criminals (Statement, April).

Computer Security Act of 1987

The Computer Security Act of 1987 (CSA) addressed security practices at government agencies. Its stated purpose is "improving the security and privacy of sensitive information in Federal computer systems," and it "creates a means for establishing minimum acceptable practices for such systems" (Computer Security Act, sec. 2). The CSA named the National Bureau of Standards as having responsibility for the establishment of standards for Federal computer systems. It also required all operators

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

of these systems to establish security plans, and called for training of their managers and users.

Presidential Decision Directive 63

President Clinton addressed the need for infrastructure protection in his Presidential Decision Directive 63 (PDD63). Although not actually legislation, this directive is included here because of the role that it plays in specifying the responsibilities of government agencies in protecting our infrastructure. The goal of PDD63 was to "achieve and maintain the ability to protect our nation's critical infrastructures." Knowing that it is essentially impossible to avoid all attacks, it also states that any interruptions of critical functions be "brief, infrequent, manageable, geographically isolated and minimally detrimental" (Clinton, sec. III). PDD63 also authorized the FBI "to expand its current organization to a full-scale National Infrastructure Protection Center (NIPC)" which "shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity" (Clinton, sec. VIII). It also authorized the creation of a private sector Information Sharing and Analysis Center (ISAC). PDD63 acknowledged that it would take a public-private partnership to adequately protect our critical infrastructure, and outlined a structure for coordinating this partnership.

Homeland Security Act of 2002

On September 20, 2001, President Bush announced the creation of a cabinet-level Office of Homeland Security in response to the September 11 attacks. This became the Department of Homeland Security (DHS) with the passage of the Homeland Security Act of 2002. DHS is composed of 22 separate agencies organized into four major directorates: Border and Transportation Security, Emergency Preparedness and Response, Science and Technology, and Information Analysis and Infrastructure Protection (DHS Agencies). The primary mission of DHS includes preventing terrorist attacks within the United States, reducing vulnerability to terrorism, and minimizing damage and assisting in recovery from attacks that may occur (Analysis 2).

USA PATRIOT Act

Little over a month after President Bush's speech in which he announced the creation of the Office of Homeland Security, the president signed the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism). Congress passed the act in response to the terrorist attacks of September 11, 2001. This act, among other changes, modifies some of the previously existing laws governing electronic evidence gathering to ease the restrictions on investigations for both domestic and foreign surveillance within the borders of the United States (USA Sketch 1).

Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime was the first international treaty dealing with computer crime (30 States). Its intent is to establish a common set of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

policies on computer crime throughout the international community. Signatory states are expected to pass domestic legislation addressing computer crime. This includes laws covering illegal access of a computer system, unauthorized modification or destruction of data, interception of network traffic, and even the production, sale, or distribution of computer programs intended to be used to commit these offenses. It also addresses issues such as child pornography, copyright, search and seizure of computer equipment and data, cooperation between parties on criminal investigations, and extradition (Convention). On November 23, 2001, representatives of 26 Council of Europe member states and four non-member states that took part in its drafting, including the United States, signed the Convention (30 States).

There have been many laws passed and directives and executive orders issued over the last several years that attempt to keep up with changing technology and address the vulnerabilities that our increasing dependence on computer networks and the Internet have introduced. But our infrastructure will remain at risk if these safeguards are not heeded and properly implemented.

Implementation Issues

After the laws are enacted and the directives issued, agencies must begin the implementation process. Policies may require that they be applied across multiple government agencies, possibly involving the private sector, as is the case with PDD63. If these policies are not very specific, interpretation and implementation may vary widely from one agency to another. On the other hand, if they are too specific, implementation may become so difficult that any necessary changes are made slowly, if at all. Unless given the appropriate priority, changes may never be implemented.

Audits of several government agencies over a five year period showed that significant weaknesses in their computer systems were seen time and again (Critical 5-6). These weaknesses were similar from agency to agency, and are typical of those that security professionals warn against. They included weaknesses in security plans, access controls, application and system software change controls, segregation of duties, and service continuity controls such as backups and recovery plans (Critical 10-17).

Implementation of the guidelines laid out in PDD63 was also reviewed, and found to be lacking in many areas. Critical infrastructure protection cannot be accomplished without performing an analysis of the systems involved so that interdependencies can be determined. If a component is highly dependent upon another system, then this must be taken into consideration when determining which systems should be protected as part of our critical infrastructure. Results of this analysis can also be used to determine which services are most critical, and therefore require the most attention and the first addressed during a recovery situation. Government audits found that in many cases this analysis had not been completed, and interdependencies had not been determined (Critical 27).

Private sector organizations also had reservations about issues such as information sharing and vulnerability reporting. Sharing information between partners might be viewed as a violation of antitrust laws. They also feared that confidential information might be released to the public through a request under the Freedom of Information Act

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

(Critical 27). Also, the release of vulnerability or other information due to a criminal investigation and prosecution may adversely affect their businesses (Combating).

The FBI has started the InfraGard program, intended to promote security awareness and information sharing between the public and private sectors. One of the reasons companies hesitate to report network intrusions is because a criminal investigation can be intrusive and costly. Members of the InfraGard program can share information in a secure, and off-the-record, format. Of course, the FBI can and will get involved when asked, but the intent is to allow the sharing of information without the worry of initiating an investigation. The FBI also offers, as an added benefit to members, computer security related tips, alerts, and training (Combating).

Law Enforcement Issues

To effectively protect our computer systems, law enforcement must be able to catch and prosecute the bad guys. They have been faced with many challenges in investigating and prosecuting cybercrime, including those due to legal and technical issues. Laws have not kept up with the technology, many times tying law enforcement's hands. As technology has advanced, these challenges have multiplied. It was hard enough to keep up with new technologies when it was just the POTS, but newer technologies such as the Internet have brought with them new hurdles for law enforcement.

One example of existing legislation affecting the ability of law enforcement to do its job came about with the advent of cable Internet connections. Telephone service and Internet access have been covered by one set of laws, while the Cable Act covered cable service. Law enforcement has used two statutes to intercept telephone and Internet communications. The pen register and trap and trace statute (pen/trap) covers interception of phone number and e-mail address information, but not content. The wiretap statute covers actual phone conversations and e-mail content. Since some customers do not use their true identity when signing up for services, billing information from these services is also valuable in tying the service to the subscriber's true identity. The Cable Act was very restrictive when it came to law enforcement access to cable company records. These restrictions, due to inconsistencies between the laws covering the different technologies, caused some cable companies to refuse access to any information under the pen/trap statute. The Act required the cable companies to notify the customer before giving out any information. The customer then had the right to be present in the courtroom when the government was providing justification for why the records were required. It's just a little hard to conduct an effective investigation when the subject of the investigation knows he is being scrutinized. The USA PATRIOT Act fixed this problem by applying the Internet access laws to cable communications services (Field sec. 211).

Another barrier that the USA PATRIOT Act addressed is the pen/trap statute itself. Before USA PATRIOT, pen/trap orders could only be applied within the jurisdiction of the court that issued them, therefore limiting jurisdiction to the local communications carrier. A communication may pass from carrier to carrier along its route from source to destination. To obtain information about both the source and destination meant that multiple court orders in different jurisdictions had to be acquired. Sometimes this meant

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

that the law enforcement agent would serve the order to the local carrier, who would then tell the agent which carrier was next in the link. Another order would then be required to determine the next carrier in the link, and the process continued until the destination was determined. Getting a court order at each point along the way wasted valuable time and resources that could be better spent in other pursuits. USA PATRIOT changed the statute to allow one court order to be applied nationally. Consider a communication that passes from the local carrier at the source, through a long-distance carrier, and finally passed to the local carrier at its destination. The agent can now obtain a single court order that can be served to, and legally binding on, all carriers in the chain (Field sec. 216 par. B).

The rapid advances in technology have also hampered law enforcement. The days of attaching a couple of wires to the phone line to listen in on conversations have long since passed. Of course, law enforcement does have some tools at their disposal such as the FBI's DCS1000, formerly known as CARNIVORE. This tool works much like commercial sniffers, but was created with law enforcement in mind and is highly configurable, able to capture only the network traffic specified in the court order while filtering out the rest (CARNIVORE). Many times the ISP gets involved in extracting the data, such as e-mail addressing information, and supplying it to law enforcement agencies. If the ISP either cannot or will not provide it, the FBI can connect CARNIVORE to their network to retrieve the data that they seek (Statement, July). State and local law enforcement agencies may not have access to such exotic tools. Even if they do, they may lack the training to know how to use them.

Law enforcement can obtain and use the same tools as any other security professional, but these tools are typically geared to the commercial market rather than to the needs of law enforcement agencies. Surveys show that the tools currently available to law enforcement agencies do not completely meet their needs. Sometimes the needed tools are not available. Common complaints about tools in use are that they lack needed functionality, are too expensive, take too much training to use, and are not geared towards the needs of law enforcement. Often these tools are used by people with a wide range of skill levels, and typically can't be adapted to match the user's abilities. This can be a problem when the levels of expertise of the investigators vary widely. This is also illustrated by the situation in which an investigator uses a tool to perform forensic analysis, and the same tool is then used by the prosecuting and defense attorneys, who may know little about the technical details, to view the results (Law).

Analysts also cite a lack of automated capabilities in these tools. They seem to be particularly dissatisfied with the tools available for performing log analysis, and report that almost one fourth of their time in the course of an investigation is spent analyzing log files. They indicate that filtering on the logs of interest, having to deal with large sets of files, and working with multiple log files, especially from multiple platforms in different formats, are tasks that are particularly problematic (Law 25-26).

Other obstacles involve a variety of areas. The cost involved in storing huge amounts of data, and ensuring its integrity, from the time of an investigation until all appeals have been exhausted years later, can be significant. Investigators may be fighting against system administrators who may be either directly responsible for the attack or are

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

protecting someone else. An investigation can easily cross jurisdictional boundaries, which means that one or more other agencies may need to get involved. The supporting agency may not be able to give the investigation the same priority, adding time to a time-critical process. This problem just gets worse if this jurisdictional boundary is a national one.

Privacy Issues

The checks and balances within our system of government were intentionally put into place to protect the rights of citizens. The Fourth Amendment contains safeguards to prevent governmental intrusions into our privacy. The wiretap and pen/trace statutes that govern interception of communications contain language that go over and above the Fourth Amendment requirements (Statement April). But there remain many doubts that government has our best interests in mind concerning rights to privacy. Some of the objections seem alarmist, but others contain valid concerns about government intrusion on privacy rights.

For example, there have been reports of an FBI project called “Magic Lantern,” to be used to capture Internet communications. This project reportedly includes the capability for the FBI to install keystroke-logging software on a suspect’s computer via a virus, therefore not requiring physical access to the computer. Of course, this would require anti-virus software to know and ignore these virus signatures so that the suspect would have no knowledge of the installation of the keystroke monitor. Although interceptions such as these require court orders, concerns that these rules are not always followed or that these orders may be too easily acquired continue (FBI Seeking).

Concerns have also been raised that the FBI is planning to force a change to the architecture of the Internet to route traffic through central servers to make it easier to monitor e-mail communications (FBI Seeking). This may be pure paranoia, but a precedent has already been set for forcing changes in network equipment. The Communications Assistance for Law Enforcement Act (CALEA) of 1994 requires telecommunications carriers to make modifications to their equipment design to allow law enforcement to be able to perform electronic surveillance (Communications).

Many call into question the provisions in the USA PATRIOT Act. This legislation was introduced shortly after the September 11, 2001 attacks and was signed by the President on October 26 of the same year. There are concerns that this bill was rushed through Congress as a knee-jerk reaction to the attacks, and was passed with little debate, even though it makes “sweeping” changes to laws dealing with privacy of Internet communications. Questions have been raised as to whether sections of this Act effectively do an end-run around protections put forth in the Fourth Amendment (USA Analysis).

There are also many concerns about the Council of Europe Cybercrime Convention. Some believe that the Convention is too vague in places and, since each signatory state is to enact its own domestic legislation, allows for wide variation in legislation dealing with such issues as human rights. The Article dealing with search and seizure of stored computer data contains language requiring “any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data”

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

to supply this information to law enforcement (Convention art. 19). The question has been raised as to whether or not this would require the disclosure of decryption keys, thereby doing away with the protections against self-incrimination (Draft).

Conclusion

Given the amount of attention that has been placed on the war on terrorism and the need for protection of our infrastructure, there appears to be a desire on the part of government to make the changes necessary to reach this goal. We have discovered many problems in our attempts to put the necessary structures and procedures in place to protect our infrastructure, sometimes seeing the same one over and over again, but these problems are not insurmountable and we must continue improving the process. We have also seen many successes, including the realization of the need for the necessary laws and coordination not only on the domestic level, but also internationally. With the changing face of technology, this is a fight that will never be completed, and we will never be able to sit back and conclude that it is done. It is a task that will continually need to be reviewed and updated. Only time will tell whether we have the determination, and the collective attention span, to carry it through.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Analysis for the Homeland Security Act of 2002. <http://www.whitehouse.gov/deptofhomeland/analysis/hsl-bill-analysis.pdf>

United States Federal Bureau of Investigation. CARNIVORE Diagnostic Tool. <http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm>

Critical Infrastructure Assurance Office. White Paper. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 1998 <http://www.ciao.gov/resource/paper598.html>

The Plain Dealer. "Combating Cybercrime: FBI's InfraGard Program Promotes Security Awareness." November 4, 2002 (available through the InfraGard website) <http://www.infragard.net/library/ig_promotes_awareness.htm>

United States Department of Justice. Federal Bureau of Investigation. CALEA Implementation Section. Communications Assistance for Law Enforcement Act (CALEA). February 6, 2001 <http://www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm>

Critical Infrastructure Assurance Office. Computer Security Act of 1987 Public Law 100-235 (H.R. 145). January 8, 1988 <http://www.ciao.gov/resource/computer_security_act_of_1987.html>

Council of Europe. Convention on Cybercrime. November 23, 2001 <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

United States Government Accounting Office. Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks. September 26, 2001 <http://www.gao.gov/new.items/d011168t.pdf>

Dartmouth College. Institute for Security Technology Studies. Cyber Attacks During the War on Terrorism: A Predictive Analysis. September 22, 2001 <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>

National Infrastructure Protection Center. Cyber Protests: The Threat to the U.S. Information Infrastructure. October 2001 <http://www.nipc.gov/publications/nipcpub/cyberprotests.pdf>

Department of Homeland Security. DHS Organization. DHS Agencies. <http://www.dhs.gov/dhspublic/display?theme=13>

Privacy International. A Draft Commentary on the Council of Europe Cybercrime Convention. October 2000 <http://www.privacyinternational.org/issues/cybercrime/coe/analysis22.pdf>

US Department of Justice and US Government Abuse Watch. FBI Seeking Tools to Control and Censor Internet. December 12, 2001 <http://www.dojgov.net/USDOJ_Carnivore_Scam.htm>

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Dartmouth College. Institute for Security Technology Studies. Law Enforcement Tools and Technologies for Investigating Cyber Attacks. June 2002 <http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf>

United States Department of Justice. Computer Crime and Intellectual Property Section (CCIPS). Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001. November 5, 2001 <http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm>

United States Department of Justice. Statement of Kevin V. Di Gregory Deputy Assistant Attorney General United States Department of Justice Before the Subcommittee on the Constitution of the House Committee on the Judiciary on the Fourth Amendment and the Internet. April 6, 2000 <http://www.usdoj.gov/criminal/cybercrime/inter4th.htm>

United States Department of Justice. Statement of Kevin V. Di Gregory Deputy Assistant Attorney General United States Department of Justice Before the Subcommittee on the Constitution of the House Committee on the Judiciary on "CARNIVORE" and the Fourth Amendment. July 24, 2000 <http://www.usdoj.gov/criminal/cybercrime/carnivore.htm>

Council of Europe. 30 States Sign the Convention on Cybercrime at the Opening Ceremony. November 23, 2001 <http://press.coe.int/cp/2001/875a(2001).htm>

Electronic Privacy Information Center (EPIC). Analysis. The USA PATRIOT Act. Last Updated March 19, 2003 <http://www.epic.org/privacy/terrorism/usapatriot/>

Library of Congress. Congressional Research Service. American Law Division. The USA PATRIOT Act: A Sketch. By Charles Doyle. April 18, 2002 (available through the U.S. Department of State, Foreign Press Centers website) <http://fpc.state.gov/documents/organization/10091.pdf>

Other Interesting Web Sites and Documents

The Terrorism Research Center <http://www.terrorism.com>

United States Department of Homeland Security <http://www.dhs.gov/>

United States Department of Justice <http://www.usdoj.gov>

United States National Infrastructure Protection Center (NIPC) <http://www.nipc.gov/>

United States Critical Infrastructure Assurance Office (CIAO) <http://www.ciao.gov/>

Center for Strategic and International Studies. Cyber Threats and Information Security: Meeting the 21st Century Challenge. By Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardas, and Michele M. Ledgerwood. December 2000 <http://www.csis.org/homeland/reports/cyberthreatsandinfosec.pdf>

The White House. Defending America's Cyberspace: National Plan For Information Systems Protection. Version 1.0. 2000 <http://www.ciao.gov/resource/np1final.pdf>

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The White House. The National Strategy to Secure Cyberspace. February 2003. <http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf>

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 25th, 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