Global Information Assurance Certification Paper

Beyond Conventional Terrorism… The Cyber Assault

By
Rajeev C. Puran
SANS GIAC Security Essentials Certification (GSEC) v1.4b
02/28/2003

Abstract

The text presented in this practical write up is established to review the various intents, events, acts and possibilities of computing technology based terrorism and warfare. This paper will look at the broad range of cyber-terrorism and warfare as well as some intricacies. Cyber-terrorism is not necessarily a new frontier however today it is more eminent than ever. Cyber-terrorism has become a new vehicle for destroying economic, political, and sociological structures.

As computers and networks become the very lifeline for every day function in America and abroad, there in lies a new avenue of exploitation by cyber-terrorists. This paper will look at environments that pose the greatest risk, profile information of who may be a threat, preventative measures and general classifications of attacks and the dangers that such attacks pose. It will briefly address the possibilities and links to human casualties of a cyber attack.

Introduction

Many Americans as well as those throughout the world that were glued to their radios, televisions, and web browsers, bared witness to a tragic and diabolical series of events on September 11th, 2001. The moniker of 9-11 will live on as the worst act of terrorism ever committed on any soil. As time progressed the public became more and more aware of the crime, the terrorists, the organization and the vehicle for such a calculated attack.

Terrorism is not a new method of criminal intent. It is know that terrorism goes as far back as ancient Egypt during the rule of the pharaohs. Today however terrorism ***can be defined as the use or threatened use of force against civilians or political figures in order to force change in a politics, government or religious factions using fear and mayhem as the primary catalyst*** [1]. We associate kidnapping, hijackings, bombings, and assassinations as the prime delivery mechanism for such acts and atrocities, leaving a gap in what we understand to be terrorist acts. There is one very important mechanism that is just beginning to come to light in the media, the enterprise community and the general public.

Cyber-terrorism and cyber-warfare have now begun to surface as a very legitimate and eminent threat to America and its allies. Cyber-warfare or terrorism goes far beyond destroying targets at a surface level. Cyber threats can be calculated to destroy the economic status and operation infrastructures of a nation that relies on computing technology for most of its, Economic Asset Management, Energy Commissions, Security and Military Assets, Transportation, Medical Facilities, Banking, Commerce and Trade, and other Vital Human services. An attack on these structures, which results in the breakdown or even temporary failure of its function, can cripple a nation psychologically, physically, and economically when the entire spectrum is considered [2]. Cyber-terrorism is a forced to be reckoned with and should, in all areas using technology as the main backbone and driver for its existence, be considered a destructive entity.

As the conventional weapons arsenals of terrorist grow, so does the intelligence arsenal they possess. It is a myth to believe that terrorists are a group of individuals that are like the cowboys of the old western era that, used simple methods, to rob banks, commit crimes against ordinary individuals, and used just a horse and a six shooter to get by. As simple as some of the more recent attacks have been, their planning and careful execution has been anything but primitive. Many terrorists are now well funded by leaders that have joined to support their cause. This in turn paves the way for more attacks to be masterminded and executed behind the cover of such devices as a laptop or a PDA.

---

1. Next Generation Terrorism Analysis, “Definitions”, 1996-2000 Terrorism Research Center, Inc. http://www.terrorism.com/terrorism/def.shtml

2. Devost, Matthew G. and Pollard, Neal C., “Taking Cyber-Terrorism Seriously”, June 27, 2002 http://www.terrorism.com/analysis/cyberterrorism-june2002.pdf

Cyber-Terrorism Dissected

As we advance into the next technological phase of trade, work, life, entertainment, medicine and sustainability we will see more and more computers and networks no matter how great or small being implanted into our environments. The information age has become the norm and the necessity. As enterprise level computing and end users face the current bombardment of viruses, worms, denial of service, man in the middle and various other attacks, investigative procedures are deployed to determine the source and intent of such efforts committed by individuals or groups.

Some perpetrators in essence are revealed to be the just the kid next door trying to cause mischief. This was evident in the case of a 15 year old youth in Montreal, known as "Mafiaboy", that caused several major web sites such as CNN, Yahoo, and Excite, to name a few, to become inaccessible [3]. As simple as the attack was it still created chaos for the groups that supply many internet and information services via their websites. The more glamorous of the hacks however belong to the ever famous, Kevin Mitnick. Mitnick went on a hacker excursion creating havoc for several phone companies, The Digital Electronics Corporation and the home computer of hacker extraordinaire and Computer Security Specialist, Tsutomu Shimomura [4]. His actions became the priority of several law enforcement agencies which divested much time and efforts from other criminals to catch him. The costs of his actions were severe but not enough to force the shutdown of any of the corporations he targeted.

The efforts that these individuals put forth could be considered cyber-terrorism in many ways. They did after all create chaos and mayhem. However they are not to fall under the category we are discussing because their actions were not deemed as threatening to change political or foreign policy or to create fear but rather to create mischief and notoriety. A cyber-terrorist threat or attack relies on the use of known attack methods and destructive data and models to force complete or temporary loss. This loss has the intent of creating a chain reaction of events.

Though many will argue that cyber-terrorism is a merely another vehicle for propaganda and the government's ploy to create fear amongst the general public, there have been several cases which clearly demonstrate that the threat is very real and the ability to carry out the act is real. It has been seen that corporations, private and public infrastructures and commerce have been victimized by everyone from young kids armed with a computer to veteran hackers with extensive cyber-tools. If the means of the attack have been useful for these individuals imagine the possibility it can have for the terrorist with motives of catastrophic nature.

Characteristics of Cyber-Terrorism

Cyber-terrorism has several distinct characteristics. These characteristics help to better differentiate the fine line between a cyber-terror attack versus a cyber attack or activities of a hacker. Cyber-terrorism will and may display the following signs:

**Remember, just because an individual or group commits a crime qualifying its actions as a cyber-based hack or attack activity, the perpetrator is not considered a cyber-terrorist unless they meet the criteria in which it is defined.*

- Attack is predefined and victims are specifically targeted
- Attack has an objective to destroy or damage specific targets such as political, economic, energy, civil and military infrastructures
- Attack may even target specific opposing religious group's information infrastructures to insight religious pandemonium
- The purpose of any attack is to create fear of the group's intentions and further their own political agenda or goals or gain fellowship by succeeding in their attacks
- Destroy the enemy's capabilities to further operate or operate within their own arena
- Persuade others to believe that the victim or victims are vulnerable and their stability negligent
- Create increased loyalty and pride within the group based on their successes [5]

Attack Methods and Deployment Strategies

- **Viruses, Worms and Trojan Horses** [6]
  - Highly prevalent or common
  - Impact is eventual and timelier than instantaneous in most cases
  - Variants include: Klez, Nimda, Code Red, Melissa, Back Orifice, or other Backdoor. Trojans
  - Common distribution is through e-mail or ftp transactions, media sharing, or hidden in code within a website
  - Attack Vectors: Boot Sector, File Infectors, Master Boot Records, Macro infections
  - Damage: Lost records, Deleted system files, corrupted system or data files, Distribution of private information, Password Recon or Theft
  - Can be very costly due to outages

- **Distributed Denial of Service (DDoS) Attacks** [7]
  - Executed in order to shutdown traffic to and from a specifically targeted system
  - Renders the target system unavailable to both internal and external users
  - Likely Targets: Banks, Trade Organizations, Information Centers, Communication Groups and some Government Entities
  - Attack Vectors: Protocol Attack, Brute Force Attacks, Continuous Rate Attacks, Variable Rate Attacks
  - Varying Degrees of Attack Delivery: Manual, Semi-Automatic and Automatic
  - Result in monetary damages can be very high due to outages

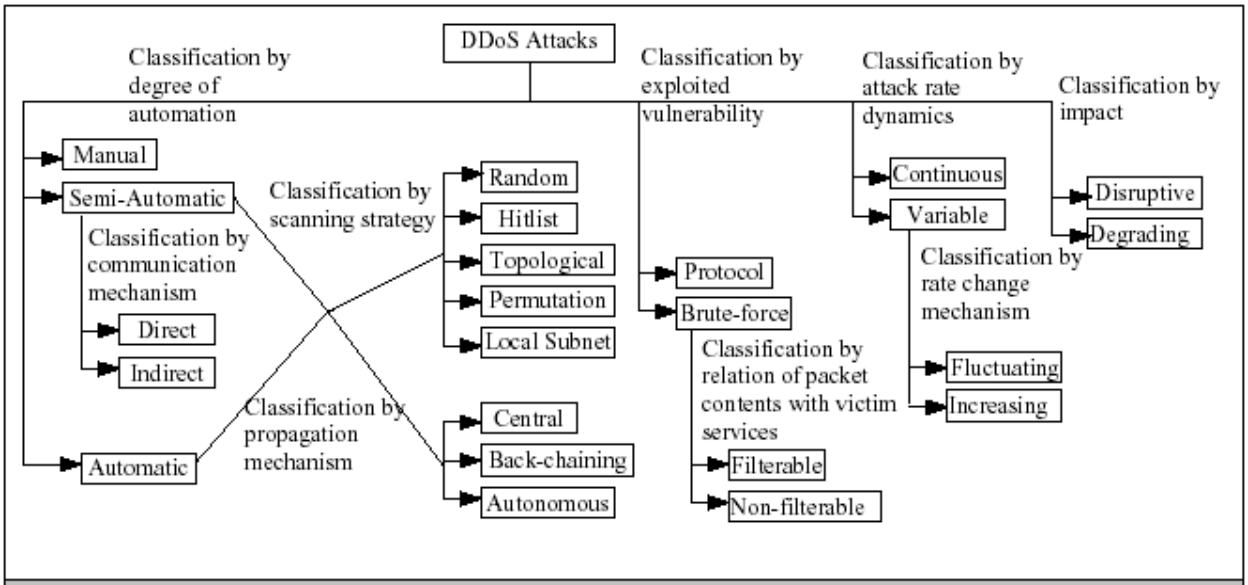

Figure 1: Taxonomy of distributed denial-of-service attacks

* "Taxonomy of DDoS Attacks and DDoS Defense Mechanisms" - Jelena Mirkovic, Janice Martin and Peter Reiher

- **Unauthorized Intrusions**
  - Intrusion Categories: Network Based Intrusions, Host Based Intrusions, Communication Eavesdropping and User Information or Database Intrusions
  - Intruder can perform malicious attacks on entire Network Systems, Clients, Communications Devices, Databases, Personal Information, Identity Theft, Financial Fraud and Espionage and Reconnaissance of Vital Information with the intent to use the information as a tool for terror
  - Likely Targets: Large Corporations, Military Suppliers and Information Systems, Weapons Systems Groups, Energy Groups and Government Institutions
  - Attackers may have first-hand knowledge of targets.
  - Attackers may be internal as well as external
  - Common Intents: Recon, Espionage and Identity Theft

- **Web Defacements and Semantic Attacks** [8]
  - Intent: Create Political Propaganda based attacks or deface a website to make a political statement
  - Launched primarily at Government Organizations, Media Groups, Religious Groups and Affiliated Businesses.
  - Common Method of Attack: Vulnerabilities to websites or servers can open doors to the file systems of such sites allowing the attacker to plant code or files or vandalize the existing files.
  - Examples are available at: http://www.attrition.org/mirror/attrition

- **Domain Name Service (DNS) Attacks**
  - Successful attack can cause a breakdown in the identification, addressing or routing of internet based systems
  - The impact of such an attack can cause internet dependent systems to be rendered unreachable.
  - Information and data infrastructures may not be able to communicate over internet communication channels
  - Commerce, Energy, Military, Transportation, Civil Services, and Media Services may be denied access to.
  - Can route connections to counterfeit or incorrect websites
  - Can be very costly due to outages
  - Linked to Denial of Service Attacks, Domain Hijacking and Cache Poisoning

---

3. Wyatt, Nelson, "CNEWS Article", April 19, 2000
http://www.canoe.ca/TechNews0004/19_hacker.html

4. Shimomura, Tsutomu, "Catching Kevin", Wired Magazine, April 19, 2000
http://www.wired.com/wired/archive//4.02/catching.html?person=kevin_mitnick&topic_set=wiredpeople

5. Axelrod, C. Warren, "Security Against Cyber Terrorism" Pershing Div. DLJ Securities Corp. Feb. 27,2002
http://www.sia.com/iuc2002/pdf/axelrod.pdf

6. Symantec Corporation – Security Response Virus Encyclopedia
http://securityresponse.symantec.com/avcenter/vinfodb.html
http://service1.symantec.com/SUPPORT/nav.nsf/docid/1999041209131106

7. "Taxonomy of DDoS Attacks and DDoS Defense Mechanisms" - Jelena Mirkovic, Janice Martin and Peter Reiher -
http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf

8. "Prevent Web Site Defacement" – Dr. Yona Hollander - December 2000
http://www.entercept.com/ricochet/articles/2000HollanderDefacement.pdf

Cyber-Terrorism and Protest Activities in Retrospect

Middle East Tension Sparks Cyber Attacks

With the Middle East Conflict at a very heated moment between bordering countries Pro-Palestinian and Pro-Israel Cyber Groups have been launching an offensive against websites and mail services used by the political sectors the opposing groups show support for. The attacks had been reported by the NIPC (National Infrastructure Protection Center) in October of 2000 to U.S. Officials. The attacks were a volley of e-mail floods, DoS attacks, and ping flooding of such sites as the Israel Foreign Ministry, Israeli Defense Forces, and in reverse, sites that belonged to groups such as Hamas and Hezbollah [9].

Pakistan/India Conflict

As tensions between the neighboring regions of India and Pakistan over Kashmir grew over time, Pro-Pakistan cyber-terrorists and recruited hackers began to target India's Internet Community. Just prior to and after the September 11th attacks, it is believed that the sympathizers of Pakistan (which also included members of the Al Qaeda Organization) began their spread of propaganda and attacks against Indian Internet based communities. Groups such as G-Force and Doctor Nuker have defaced or disrupted service to several major entities in India such as the Zee TV Network, The India Institue of Science and the Bhabha Atomic Research Center which all have political ties. The Group, Pakistani Hackerz Club also went as far as to target the United States Air Force Computing Environment and the Department of Energy's Website [10].

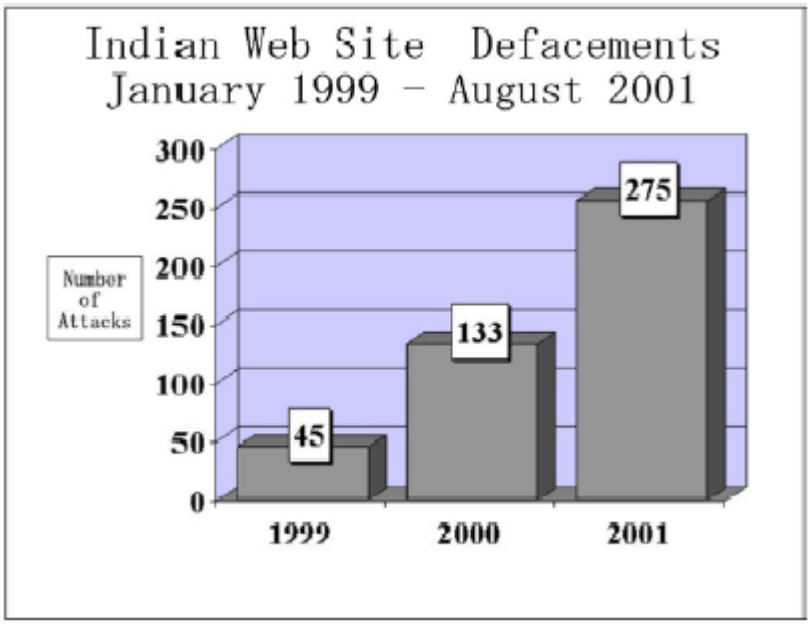

Figure 1
"Cyber Attacks During the War on Terrorism" India/Pakistan Conflict
Institute for Security Technology Studies – Dartmouth College
Vatis, Michael A – September 22, 2001

Retaliation in China

In May 1999 the accidental bombing of a Chinese embassy in Yugoslavia by U.S. Bombers, led to a massive web site defacement and e-mail bombardment attack on American companies and agencies. Pro-Chinese hackers and political groups executed the attacks to gain sympathy for the Chinese cause.

US Government sites such as the U.S. Departments of Energy and the Interior, and the National Park Service were all hit and had web sites defaced along with the White House web site. The site was downed for three days by continual e-mail bombing. Although the attack was rather random and brief and affected a small number of U.S. sites, the effects could have been worse [11].

Tamil Tiger Attempt

In 1998, with surges of violence committed in Sri Lankan over several years, attacks in cyber-space were the next area to target. The group known as the Tamil Tigers, a violent guerrilla organization, bombarded Sri Lankan embassies with over 800 e-mails a day. This was carried out over a two week period. The attacked the e-mail message conveyed the message, "We are the Internet Black Tigers and we're doing this to disrupt your communications." After the messages created such major disruption the local Intelligence authorities were dispatched to investigate. The authorities declared the attack as the first known attack on the Sri Lankan by the terrorists on any computer system in the nation [12].

---

9. "Middle East E-mail Flooding and Denial of Service (DoS) Attacks" – National Infrastructure Protection Center – October 26, 2000http://www.nipc.gov/warnings/assessments/2000/00-057.htm

10. Cyber Attacks During the War on Terrorism" India/Pakistan Conflict Institute for Security Technology Studies – Dartmouth College Vatis, Michael A – September 22, 2001
http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf

11. Cyber Protests: The Threat to the U.S. Information Infrastructure - October 2001
http://www.nipc.gov/publications/nipcpub/cyberprotests.pdf

12. Cyber Terrorism – "Testimony before the Special Oversight Panel on Terrorism" – Dorothy E. Denning – May 23, 2000
http://www.terrorism.com/documents/denning-testimony.shtml

A National Defense Initiative

Cyber or Technology based crimes have long been a concern for authorities both in the Untied States and abroad. From World War II to the Cuban Missile Crisis to Operation Desert Storm and now the War against Terror, cyber-warfare and terrorism has been a critical factor in one form or another. Protecting a nation such as the United States from any form of cyber-based warfare or terrorism is not a task of simple intervention. It is more a practice of cause and effect. A planned and surgically implemented computing infrastructure protection system can be a very complex beast. Now a hotbed cyber threats are being handled by different agencies with a united front. Most of these agencies now are joined together as a part of the ***Homeland Security Initiative*** [13].

NSA- National Security Agency

- Established in 1952 with the establishment of the Central Security Service (CSS) in 1972
- Provides signals intelligence and communications security efforts for the United States
- The Nation's key cryptologic organization

FBI – Federal Bureau of Investigations

- Federal Law Enforcement Branch
- Specializes in White Collar and High Tech Crimes

NIPC - National Infrastructure Protection Agency

- Joint venture including the two agencies
- Focal point for threat assessment, warning, investigation, and response for threats or attacks against critical infrastructures
- Department include: Information Analysis and Infrastructure Protection Directorate
- Provides law enforcement and intelligence information and reports to relevant federal, state, local agencies, and private sectors

CIAO - Critical Infrastructure Assurance Office

- Created in May 1998 to coordinate the Federal Government's initiatives on critical infrastructure assurance
- Coordinate and implement the national strategy
- Assess the U.S. Government's own risk exposure and dependencies on critical infrastructure
- Raise awareness and educate public understanding and participation in critical infrastructure protection efforts
- Coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors

---

13. The National Strategy to Secure Cyberspace – Homeland Security Initiative
http://www.whitehouse.gov/pcipb/

Prevention Techniques and Practices

Corporate or Business Level Preparedness

Keeping a corporate or information welfare group intact and functionally protected from cyber attacks takes careful implementation of security policies, procedures and tools. The following are key highlights of an intermediate plan of defense.

- ✓ Develop a Protection and Risk Assessment and Mitigation Plan
- ✓ Investigate vulnerabilities and attack vectors that may exist in the company infrastructure
- ✓ Engage with CERT or Security Assessment Groups for advisories and methods
- ✓ Ensure Network Security with Firewall Systems and Border Routers
- ✓ Use Secure Authentication practices for key Administration Areas (WAN, LAN, Routing, Servers, Clients)
- ✓ Strong and regularly updated Anti-Virus Software deployments
- ✓ Include Security Monitoring or Intrusion Detection Analysis and Tools in operations: Network Based or Host Based
- ✓ Configure and employ proper Filtering methods with IDS systems (Ingress and Egress)
- ✓ Regular Audit of Environment for non-secure systems or devices for risks and vulnerabilities
- ✓ Keep up to current on all necessary security patches recommended by Risk Assessment Bureaus, Systems and Software Vendors.
- ✓ Enforce Strong Password Authentication Practices
- ✓ Implement and enforce policies that will safeguard the infrastructure and keep wholes or leaks developing from within internal channels
- ✓ Backup Vital Data and implement Fail-Over or Disaster Recovery, Business Continuity systems
- ✓ Provide education on Information Security Practices for personnel

End User or Home User Preparedness

With the advent and offerings of high speed internet into most of today's suburban and city dwellings, the risk for even the "Average Joe" residential customer or end user to become a victim. Cyber-terrorism may incorporate financial crimes and identity theft against everyday citizens. The rise in viruses and identity theft means even a personal computer at home needs to be secured from such attacks. Again these are steps that can be taken to secure the home front's computer infrastructure [14].

- ✓ Install host based firewall software or implement a hardware based router/firewall package
  - Zone Alarm, Sygate or Tiny Personal Firewall [15]
  - Linksys, Netgear, 2Wire Broadband Router w/firewall [16]
- ✓ Install Anti-Virus Software and keep signatures and operational files updated (Anti-Virus Software Vendors generally provide automatic updates capabilities)
- ✓ Use strong secure passwords that are harder to crack
- ✓ Ensure that primary and secondary users of home based systems practice safe and secure usage while on maintaining a connection to the internet.
- ✓ Understand and investigated the usage and functions of online tools and services such as Messaging, Chat Relay, and Peer-2-Peer sharing services.
- ✓ Backup up system regularly and secure critical information.
- ✓ Be aware of electronic mail or internet traffic that may be unusual or strange (i.e. mail attachments or messages)

---

14. http://www.web-centric.net/files/cybersecurity2.pdf
http://www.web-centric.net/files/cybersecurity2.pdf

15. Home PC Firewall Guide – Personal Firewall Guide
http://www.firewallguide.com/software.htm

16. Home PC Firewall Guide – Broadband Router Firewall Guide
http://www.firewallguide.com/hardware.htm

What to Expect from Here

The more individuals, businesses, government and civil services incorporate and integrate computer and network based systems into their daily functions, the more the potential for catastrophic cyber threats exist. How grand are the activities of terrorist armed with PC's, Laptops, PDA's and Cell Phones? Regardless of the potential "What If" and "It Could Happen" provocation, the need to safeguard the nation infrastructure has become a top priority item.

The potentials are great and the burden in the future can be tremendous. We have seen the effects of terrorism in tragic terms and we have seen the aftermath. The use of even e-mail to mastermind the attacks of September 11th can be deemed as cyber-terrorism. The end justifies the means. The network of individuals and the use of high tech tools have made the possibilities even greater. Securing cyber-space is an initiative that starts with the end user and systematically spreads into the big picture and the agencies commissioned with protecting it.

Many will argue that too much hype is put into such attacks on critical infrastructures and that the possibility of an occurrence is unlikely. Some will say the media and politics create paranoia to manifest control of the use of computer systems. What ever the case may be, it seems extremely necessary for such a defense capability to be in place. If the technology exists and is available, and fundamental causes and movements exist against the entities that support the technology, then more than likely the means to destroy or cripple it will exist. The result may again be devastation to life and standing economic structures of a nation; over time the blows can be fatal.

Reference

1. Next Generation Terrorism Analysis, “Definitions”, 1996-2000 Terrorism Research Center, Inc.
http://www.terrorism.com/terrorism/def.shtml

2. Devost, Matthew G. and Pollard, Neal C., “Taking Cyber-Terrorism Seriously”, June 27, 2002
http://www.terrorism.com/analysis/cyberterrorism-june2002.pdf

3. Wyatt, Nelson, “CNEWS Article”, April 19, 2000
http://www.canoe.ca/TechNews0004/19_hacker.html

4. Shimomura, Tsutomu, “Catching Kevin”, Wired Magazine, April 19, 2000
http://www.wired.com/wired/archive//4.02/catching.html?person=kevin_mitnick&topic_set=wiredpeople

5. Axelrod, C. Warren, "Security Against Cyber Terrorism" Pershing Div. DLJ Securities Corp. Feb. 27,2002
http://www.sia.com/iuc2002/pdf/axelrod.pdf

6. Symantec Corporation – Security Response Virus Encyclopedia
http://securityresponse.symantec.com/avcenter/vinfodb.html
http://service1.symantec.com/SUPPORT/nav.nsf/docid/1999041209131106

7. “Taxonomy of DDoS Attacks and DDoS Defense Mechanisms” - Jelena Mirkovic, Janice Martin and Peter Reiher -
http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf

8. “Prevent Web Site Defacement” – Dr. Yona Hollander - December 2000
http://www.entercept.com/ricochet/articles/2000HollanderDefacement.pdf

9. "Middle East E-mail Flooding and Denial of Service (DoS) Attacks" – National Infrastructure Protection Center – October 26, 2000http://www.nipc.gov/warnings/assessments/2000/00-057.htm

10. Cyber Attacks During the War on Terrorism" India/Pakistan Conflict Institute for Security Technology Studies – Dartmouth College Vatis, Michael A – September 22, 2001
http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf

11. Cyber Protests: The Threat to the U.S. Information Infrastructure - October 2001
http://www.nipc.gov/publications/nipcpub/cyberprotests.pdf

12. Cyber Terrorism – “Testimony before the Special Oversight Panel on Terrorism” – Dorothy E. Denning – May 23, 2000
http://www.terrorism.com/documents/denning-testimony.shtml

13. The National Strategy to Secure Cyberspace – Homeland Security Initiative
http://www.whitehouse.gov/pcipb/

14. http://www.web-centric.net/files/cybersecurity2.pdf
http://www.web-centric.net/files/cybersecurity2.pdf

15. Home PC Firewall Guide – Personal Firewall Guide
http://www.firewallguide.com/software.htm

16. Home PC Firewall Guide – Broadband Router Firewall Guide
http://www.firewallguide.com/hardware.htm